BR

CIVIL NO. _____

CRIM. NO. 05-CR-150

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

FABIO CARANI — PETITIONER

07cv7040
JUDGE GRADY
MAG. JUDGE DENLOW

-vs-

UNITED STATES OF AMERICA — RESPONDENT

MEMORANDUM OF LAW IN SUPPORT OF PETITION TO VACATE, SET ASIDE, OR CORRECT SENTENCE PURSUANT TO 28 U.S.C. § 2255

SUBMITTED PRO SE BY:

FABIO CARANI
REG. NO. 21827-424
FCI ASHLAND
P.O. BOX 6001
ASHLAND, KY. 41105

STANDARD OF REVIEW

Section 2255 authorizes a sentencing court to discharge or resentence a prisoner if the Court concludes that it was without jurisdiction to impose the sentence, or the sentence exceeds the maximum allowed by law, or the sentence is otherwise subject to collateral attack. 28 U.S.C. § 2255; United States v. Addonizio, 442 U.S. 178, 185 (1979)[citing United States v. Hayman, 342 U.S. 205, 216-17 (1952)]. A petitioner can collaterally attack his sentence under Section 2255 where the trial and/or sentencing judge made an "objectively ascertainable error." Addonizio, 442 U.S. 187.

A petitioner collaterally attacking his conviction or sentence pursuant to § 2255 bears the burden of proving his or her grounds for relief by a preponderance of the evidence. White v. United States, 352 F.Supp.2d 684, 686 (E.D. Va. 2004); Wyche v. United States, 317 F.Supp.2d 1, 6 (D. D.C. 2004); Wright v. United States, 624 F.2d 557, 558 (5th Cir. 1980); Bouchillon v. Collins, 907 F.2d 589 (5th Cir. 1990).

Being a pro se petitioner, Mr. Carani is entitled to have his petition and asserted issues construed liberally, because pro se petitioners are held to less stringent standards than attorneys drafting such complaints. Donald v. Cook County, 95 F.3d 548, 554-56 (7th Cir. 1996). Moreover, the Court must accept Mr. Carani's factual assertions as true, unless they are patently incredible or have been disputed by affidavit. Haines v. Kerner, 404 U.S. 519 (1972). However, disputed facts which are material

to the determination of Mr. Carani's claims cannot be decided on the basis of affidavits, but must be decided following an evidentiary hearing where the parties are subjected to examination while under oath. Fontaine v. United States, 411 U.S. 213 (1973).

Here, Mr. Carani's assertions of factual events outside the record of this case are not patently incredible, and they are material to the determination of his claims within this instant petition. Furthermore, within this instant petition Mr. Carani has proven his claims. Accordingly, Mr. Carani is entitled to the relief requested. Alternatively, an evidentiary hearing must be held in this matter as soon as practical.

JURISDICTIONAL STATEMENT

On June 15, 2005, a federal grand jury sitting for the Northern District of Illinois returned a three-count superseding indictment against Petitioner Fabio Carani. On September 6, 2005, after a five-day jury trial, the jury returned a verdict of guilty as to Count 1; and not guilty as to Count 3. The jury was unable to reach a decision as to Count 2, thus, the Court declared a mistrial as to that count.

The Court sentenced Mr. Carani to a 72-month term of imprisonment in the Bureau of Prisons on March 16, 2006. Mr. Carani filed a timely notice of appeal. The Seventh Circuit Court of Appeals affirmed Mr. Carani's conviction and sentence in a published opinion on July 6, 2007. [Exhibit 1]. On August 23, 2007, the Seventh Circuit granted Mr. Carani's motion to recall the mandate for purposes of his pro se petition for rehearing. [Exhibit 2]. Shortly thereafter, the Seventh Circuit denied Mr. Carani's rehearing petition. [Exhibit 3].

Because Mr. Carani is filing his motion to vacate sentence within one year of the Seventh Circuit's denial of his petition for rehearing, this Court has jurisdiction over this matter pursuant to 28 U.S.C. § 2255.

STATEMENT OF THE CASE

On February 12, 2005, a Criminal Complaint was filed against Fabio Carani based on the affidavit of Jennifer Sapper, a Special Agent with Immigration and Customs Enforcement, who stated she received an image of child pornography on May 29, 2003. [R.1].

On April 27, 2005, a Northern District of Illinois federal grand jury indicted Mr. Carani. The sole charge was knowingly possessing a computer that contained video images of child pornography, contrary to 18 U.S.C. § 2252A(a)(5)(B). [R.16]. On June 15, 2005, the grand jury returned a superseding indictment, which added two counts of knowing receipt of child pornography, relating to two computer files, contrary to 18 U.S.C. § 2252A(a)(2)(A). [R.29].

The case proceeded to a three day jury trial. The jury returned a verdict of guilty as to Count 1 (knowing possession of child pornography), not guilty as to Count 3 (knowing receipt of child pornography), and it was unable to render a unanimous verdict as to Count 2 (knowing receipt of child pornography). [R.67]. The Court entered findings of guilt, acquittal and mistrial consistent with the jury verdicts. [R.67].

Mr. Carani moved for a new trial, to arrest judgment and for a judgment of acquittal notwithstanding the verdict. [R.77]. Mr. Carani restated his objection to the issuance of a "supplementary jury instruction" in response to a jury question regarding possession and also raised additional arguments in support of the motion [R.77]. These motions were denied. [R.81].

On March 16, 2006, the Court sentenced Mr. Carani to 72 months in prison and two years on supervised release. [R. 111]. His notice of appeal was timely.

Mr. Carani is currently serving his sentence of imprisonment. On direct appeal, Mr. Carani challenged both his conviction and the sentence imposed. Specifically, Mr. Carani argued that: (1) the district court abused its discretion by giving the deliberate avoidance "ostrich" instruction to the jury; (2) the district court erred in its response to the jury's question by including the language "knew or strongly suspected;" and (3) the district court erred in applying a sentencing enhancement for distribution of child pornography.

On July 6, 2007, the Seventh Circuit Court of Appeals affirmed Mr. Carani's conviction and sentence in a published opinion. [Exhibit 1]. Mr. Carani filed a timely petition for rehearing and/or suggestion for rehearing en banc. On September 5, 2007, the appeals court denied Mr. Carani's petition. [Exhibit 3].

STATEMENT OF THE FACTS

The charges in this case relate to the use of Kazaa Lite. Mr. Carani was charged with one count of knowingly possessing a computer that contained video images of child pornography, contrary to 18 U.S.C. § 2252A(a)(5)(B) and two counts of knowing receipt of child pornography, relating to two computer files, contrary to 18 U.S.C. § 2252A(a)(2)(A). [R.16; R.29]. The government did not charge Mr. Carani with distribution of child pornography, nor did the government claim to have any information that Mr. Carani was trying to distribute child pornography. [R.131, 115, lines 19-24]. During the search of the Carani home, no hard copies of child pornography or still pictures of child pornography were recovered. [R.131, 131, lines 2-6]. There were no child pornography DVDs, VHS tapes or magazines. [R.131, 121, lines 7-14]. Likewise, there was no camera film, photos of child pornography, or child pornography mailing lists. [R.131, 121, lines 21-122-12].

On the morning of February 11, 2005, law enforcement entered the Carani home with guns drawn. [R.131, 142, line 25-113, line 2; 144, lines 20-25; 655, lines 1-7; 720, line 7-721, line 3; 722, lines 3-12].

Both Mr. Carani and his wife were interviewed by law enforcement following the execution of the search warrant. Special Agent Sapper testified that Mrs. Carani said that she had seen child pornography on the computer with her husband and that after "viewing them all the way through" they deleted them. [R.131, 124,

lines 10-25]. Special Agent Sapper also claimed that Mrs. Carani said that her husband would download child pornography and that they would view it together. [R.131, 847, lines 3-18; 847, line 25-848, line 3].

At trial, Mrs. Carani testified that she was interviewed without an interpreter by two agents. [R.131, 661, lines 8-16]. She also stated that she never told the agents that she had seen child pornography on the computer. [R.131, 661, line 17-663, line 6].

Special Agent Jarrod Winkle, also with the Department of Homeland Security ICE [R.131, 126, lines 1-10], interviewed Mr. Carani. During the first one to two hours of Mr. Carani's interview with Special Agent Winkle, Mr. Carani stated that he did not have child pornography on his computer and that he did not look at or maintain child pornography. [R.131, 151, lines 8-22; 726, lines 2-6]. Mr. Carani advised that he did not "chat" on the internet and that he had never been to a child pornography website. [R.131, 191, line 13-15; 191, line 23-192, line 1].

Mr. Carani advised Special Agent Winkle that he used Kazaa to download pornography. [R.131, 130, lines 19-20]. He indicated that he used the search terms "sex" and "lesbian" to seek out adult pornography. [R.131, 130, line 25-131, line 3; 774, lines 3-5]. Mr. Carani stated that he had come across child pornography "about ten times" while searching for adult pornography. [R.131, 131, lines 4-11; 774, lines 6-13]. He advised that he would watch the video "for a couple seconds" in order to "see what it was" and then delete it. [R.131, 131, lines 12-15; 774, lines 14-19].

According to Special Agent Winkle, he also stated that "he had seen tons of child pornography" and that he had "receive[d] at least 25 to 50 videos of child pornography." [R.131, 131, lines 19-21]. At trial, Mr. Carani disputed using the term "tons" and said that the agents suggested numbers of videos, but that he could not say a specific number. [R.131, 776, lines 10-19]. Special Agent Winkle also advised that Mr. Carani stated that "he may have one saved of a 16-year-old girl," which Mr. Carani disputed. [R.131, 131, line 22-132, line 3; 774, line 20-23]. Mr. Carani testified that he did not know how to share files and didn't know that files would be shared. [R.131, 153, lines 12-17]. Mr. Carani stated he used the computer to download music and adult pornography. [R.131, 13, lines 18-24].

According to Special Agent Winkle, Mr. Carani also reportedly stated that he had used the search terms "pedo" and "r@gold" to search for child pornography. [R.131, 133, lines 2-14]. Mr. Carani also purportedly stated that he was interested in "family incest type pornography." [R.131, 134, line 25-135, line 3]. Mr. Carani disputed this statement and said that he was describing having an adult pornographic "taboo video" from the 1970s that had an incest theme. [R.131, 776, line 22-777, line 6]. Mr. Carani stated that he "may have inadvertently shared [child pornography] via Kazaa, but never intended to." [R.131, 135, lines 16-19]. Allegedly, Mr. Carani also stated that he became interested in child pornography because "that regular sex type pornography just didn't do it for him anymore, and he started looking for new avenues." [R.131, 135, lines 20-24]. Mr. Carani denied having

made these comments at trial. [R.131, 778, lines 9-14].

Also according to Special Agent Winkle, Mr. Carani indicated that he was familiar with the files: "r@ygold," "25 pedo," "Real Kiddy Movie 6," "Preteen Blow Job," "Mom Helping Preteen to Have Sex," and other titles as well. [R.131, 136, lines 11-137, line 24]. However, the specific files names were all suggested by Special Agent Winkle, and he did not recall Carani mentioning any file names. [R.131, 160, line 18-161, line 18].

At trial, Mr. Carani stated that he told the agents that if child pornography "did come up, [he] deleted it." [R.131, 727, line 16-18; 730, lines 4-14]. Mr. Carani testified he would delete the files once he saw what it was and denied saying that he watched them for one to two minutes. [R.131, 730, lines 15-18]. He said that he told the officers that he never searched for child pornography. [R.131, 730, lines 23-24]. Mr. Carani also said that he said that he was not interested in child pornography and that he did not have any such pictures, videos or photographs. [R.131, 731, lines 6-22].

Mr. Carani also testified that he did not use search terms of "pedro" or "r@ygold" and that he did not know what the terms meant. [R.131, 731, line 23-732, line 3]. He denied stating that he had ever gone to a website dealing in this subject. [R.131, 732, lines 12-17]. Mr. Carani also denied making the statements that he was no longer interested in regular pornography or that he did not think it was a big deal to view child pornography in one's home. [R.131, 732, line 25-733, line 10].

Mr. Carani also testified that he had not see the "Baby J-

Sunshine" or "Real Kiddy Movie Young Girl Gets Fucked 12.mpg" or "Segundo" pornographic videos prior to being in court. [R.131, 713, lines 2-20; 718, line 5-179, line 8]. He said that he told the officers that he deleted any child pornography that he came across, and that he first heard the term "Segundo" when an agent used it during the interrogation. [R.131, 733, line 11-734, line 12]. Mr. Carani stated that the terms "r@ygold," "brother sister fuck," "real kiddy movie 6" were all first mentioned by the agents, and that he said that he did not know these terms. [R.131, 734, line 13-735, line 8]. He also described having had problems with the computer. [R.131, 714, line 21-717, line 25].

While in custody, Mr. Carani also prepared a written statement. [R.131, 137, lines 25-238, line 13]. This statement was written after Mr. Carani had been interviewed for "[a]pproximately six [hours]." [R.131, 202, lines 9-13]. This statement advised that:

> "I have viewed child pornography in the past and then deleted it. I have only one saved right now in the saved section, which is My Kazaa Lite. As far as computers are concerned, I am a beginner at best. I did not distribute any of these videos on purpose, and I have no explanation as to how these videos were shared, but I never shared anything. I don't even know how to do so. The only explanation is that, that so as I viewed them and deleted them, they were automatically shared without my knowing of it. Some of these videos I stumbled upon by accident downloading other videos, and through curiosity I looked up some child pornography and again deleted it when I saw it. But the more I saw, the more I felt it was wrong to do so. My intentions

> were never to hurt anybody, and forgive my ignorance, but I did not know that this was against the law via the way it was done through Kazaa Lite. I feel extremely bad about what happened, but I can say I learned a lot through this experience."

[R.131, 140, lines 6-22].

At trial, Mr. Carani advised that he signed and dated the statement. [R.131, 736, lines 19-737, line 4]. He acknowledged that he had seen and deleted child pornography. [R.131, 737, lines 7-23]. He also described writing that he had "only one saved right now" because he was told by the agent that he had a file named "Segundo" on his computer and that the agents said to just write it down despite his not having seen it and not knowing that it was there. [R.131, 737, lines 24-739, line 9; 743 line 10-744, line 4; 779, line 19-780, line 19]. Mr. Carani advised that he wrote that "through curiosity" he looked up other child pornography and deleted it, and explained that he was describing searching within the files in Kazaa Lite to determine if other such files were downloaded inadvertently. [R.131, 740, line 10-24; 782, line 24-784, line 8]. Mr. Carani stated that the comment that it "was wrong to do so" referred to viewing such images. [R.131, 740, line 25-741, line 5]. He described feeling badly about this experience because he felt that it was a signal that viewing adult pornography was morally inappropriate. [R.131, 741, line 22-742, line 5].

Mrs. Carani testified that Mr. Carani used the computer to find music files and adult pornography. [R.131, 658, lines 16-21]. She testified that he used search terms like "sex" and "adult

pornography." [R.131, 659, lines 5-6]. She stated that she and her husband viewed adult pornography together on the computer. [R.131, 659, lines 14-16]. She stated that she never saw her husband viewing child pornography, nor had she ever seen child pornography on the computer. [R.131, 659, line 20-660, line 2]. Mrs. Carani stated that her husband told her that when he would download pornography that he would select "maybe the first 20 or the next 20" files responsive to his request. [R.131, 678, line 3-680, line 5]. Mr. Carani also described downloading files in large blocs when he would come home from work and then he would check on the computer later (sometimes days later) to see which files had successfully downloaded and review them. [R.131, 706, line 12-707, line 16; 754, line 2-759, line 17; 760, line 17-761, line 4; 761, line 25-762, line 9].

Mr. Carani testified that he installed Kazaa with some difficulty and taught himself how to use it. [R.131, 701, line 2-704, line 3]. He acknowledged using the program to download classical music, rock music, and "neoclassical" guitar music. [R.131, 751, line 21-752, line 21]. Mr. Carani also sought video clips involving wrestling, ultimate fighting and adult pornography. [R.131, 752, line 22-752, line 6]. He stated he used the terms "sex," "porno," "pornography," "adult pornography," and "lesbians" to search for pornographic video. [R.131, 704, lines 4-23].

Mr. Carani testified that he was unaware of a "My Shared" folder until he was charged in this case. [R.131, 708, lines 1-9]. He also stated that he viewed files from "My Kazaa Lite" and was not aware of Windows Media Player. [R.131, 708, lines 10-19].

He stated that he and his wife had viewed adult pornography together, but that they had never viewed child pornography together. [R.131, 710, line 12-711, line 7]. He stated he was unaware of any file sharing done through his computer. [R.131, 793, lines 4-12].

Mr. Carani's computer contained video files involving rock music videos, kick boxing and ultimate fighting videos, adult pornography and "a fair amount of child pornography." [R.131, 298, line 20-25; 409, line 10-22]. One of the receipt charges related to a movie file, titled "Baby J-Sunshine," located in the temporary internet folder. [R.131, 276, line 10-280, line 8]. A video file titled "Segundo" located in the My Shared Folder of Kazaa Lite was also described. [R.131, 299, line 1-300, line 9]. The government also discussed four other videos that prosecution expert, Special Agent Skinner, believed to be child pornography. [R.131, 303, line 21-304, line 11]. The parties stipulated that these files contained sexually explicit conduct with minors. [R.131, 304, line 15-23]. All of these movie files were available to be shared through the seized computer. [R.131, 304, line 6-11].

At the time of seizure, the computer had 214 files available for sharing from the "My Shared Files" file folder. [R.131, 312, line 2-7]. These files include "lots of" music files and sports related files. [R.131, 318, line 10-319, line 7; 319, line 7-9; 364, line 10-18].

At trial, Special Agent Skinner described that other users would attempt to download from him when he tested the version of Kazaa Lite on the seized computer. [R.131, 332, line 14-19]. He

described that people would attempt to download files from him, without his taking any action. [R.131, 336, line 11-24]. He described that he had to take an action on the computer in order to prevent other users from downloading files on the computer through Kazaa. [R.131, 336, line 11-337, line 7; 338, line 14-340, line 10]. He advised that he "wasn't on the computer for more than five or ten minutes at the most before I had multiple people trying to download from me." [R.131, 339, line 22-25]. He also noted that despite cancelling the downloads multiple times that other users "keep coming back." [R.131, 340, line 1-6].

Special Agent Skinner also described evidence of a "hack" which appeared to be used to increase the participation level in Kazaa of the seized computer. [R.131, 360, line 2-24]. The hack increases the participation by having a user download files from his own computer. [R.131, 36, line 6-8]. He described that the hack was "extensively used." [R.131, 362, line 4-6]. Defense expert Scott Ellis described that the Kazaa Lite software will increase a user's participation level by automatically downloading files from a user's computer to itself. [R.131, 505, line 8-506, line 6]. He opined that the software was increasing the participation level, without user intervention, because there was no record in the internet history of the hack being typed in by a user. [R.131, 505, line 7-511, line 12]. Special Agent Skinner further acknowledged that he does not know "for sure" whether the hack was done by software. [R.131, 833, lines 6-9].

Special Agent Skinner concluded that the person using the seized computer knew how to access the My Shared Files folder.

[R.131, 371, line 23-372, line 2]. He opined that, "the person using this computer intentionally was looking for child pornography and accidentally came across adult pornography." [R.131, 373, line 13-19].

Special Agent Skinner testified that the keyword and description are available to a user on Kazaa before one selects the file for downloading. [R.131, 330, line 10-15]. However, Special Agent Skinner acknowledged that when one searched Kazaa for adult pornography that he would "get a lot of stuff" including "adults having sex with minors." [R.131, 377, line 2-16; 378, line 15-22]. Further, the computer analysis could not determine what search terms had been used on the seized computer. [R.131, 378, line 23-379, line 2]. Thus, there was no evidence that Mr. Carani had typed in the specific file names described by the government including the files that formed the basis of the charges. [R.131, 379, line 3-15].

Special Agent Skinner noted that there were 235 files in the "My Shared" folder and 124 or 128 filed in the "My Kazaa Lite" folder. [R.131, 390, line 1-16]. He agreed that there may be something wrong with the Kazaa Lite program as the number of files in both locations should be the same. [R.131, 390, line 17-391, line 7]. Defense expert Ellis concurred that Kazaa Lite was not working properly on the seized computer. [R.131, 340, line 10-16; 471, line 6-13]. Special Agent Skinner also stated that files may take days or even weeks to download and that once downloaded other users can download the files without the user's knowledge or control. [R.131, 396, line 5-397, line 12; 602, line 6-608, line 13].

Mr. Ellis described Kazaa Lite as "a piece of rogue software" that "can behave in an uncontrolled fashion." [R.131, 463, line 18-464, line 4]. He described that a user could select single files that came up in response to a search or highlight multiple files. [R.131, 465, line 19-466, line 7]. He further described that when a file is viewed through the My Shared Files folder in Kazaa Lite that a record of that action would be shown in the "recent files list" and the "IE history" or Windows media history. [R.131, 466, line 13-468, line 17]. There was no record of a child pornography file in any of these locations on the seized computer. [R.131, 466, line 20-468, line 17]. There was no evidence that Mr. Carani had ever accessed the My Shared Files folder. [R.131, 475, line 5-468, line 17; 475, line 15-476, line 11]. Mr. Ellis opined that Mr. Carani was not a sophisticated computer user. [R.131, 478, line 18-21]. He also offered an expert opinion as to whether Mr. Carani was aware of the existence of the my shared Files Folder, and opined that:

> "Well, I have no way to pry into Mr. Carani's brain, but I do have the evidence in the, on the computer that suggests he never looked at it which implies to me he didn't know it was there and, yeah, you could certainly draw that conclusion in my opinion he didn't know it was there."

[R.131, 474, line 18-23].

Scott Ellis testified that the listing of files in My Kazaa Lite was not stable and that it changed when the government agents turned on the program. [R.131, 481, line 2-483, line 16]. He also noted that the last access date of the "Segundo" file was after the

search warrant was executed. [R.131, 484, line 1-8]. He stated that a number of things could have caused this later access of the file, but that there is no way to say what had caused the access. [R.131, 484, line 9-485, line 3]. Due to this later access, there is no way to determine that "Segundo" resided in Mr. Carani's "My Kazaa Lite" prior to the search warrant being executed. [R.131, 485, line 4-11]. He also described how another file had appeared in the "My Kazaa Lite" during testing after the computer had been seized and was being examined. [R.131, 481, line 2-482, line 1; 485, line 12-15]. Special Agent Skinner stated that he did not experience a similar incident during his testing of the computer. [R.131, 825, lines 19-827, line 5].

"Baby J Sunshine" was another file that contained child pornography that was found in the temporary internet file. [R.131, 485, line 16-486, line 6]. Mr. Ellis defined a temporary internet file as an automatic download of graphic contents of a website. [R.131, 486, line 11-22]. Mr. Ellis defined the file created, last written and last accessed dates. [R.131, 487, line 16-489, line 11]. He defined creation date as when a file arrived on the computer and began to download; last written as when the download completed, and last access as "the last time that anything touched the file." [R.131, 487, line 21-489, line 5]. Mr. Ellis made clear that last access does not necessarily mean the last time the file was viewed. [R.131, 489, line 6-11].

The "Baby J Sunshine" file had an identical last written and last access time stamp meaning that the "last thing to touch the file was the operating system when it finished downloading it."

[R.131, 490, line 2-491, line 3]. He also described a second "Baby J Sunshine" file had the same last access and last written time stamps "[d]own to the second" leading Mr. Ellis to conclude that "a human did not download these files" and that Mr. Carani was not on the Internet at the time the file was downloaded. [R.131, 491, line 20-492, line 6; 494, line 12-24]. He opined that both were ".dll" files which is a security flaw that allows somebody who is remotely connected to the computer to download files. [R.131, 492, line 7-14; 631, line 9-632, line 16]. he concluded that Mr. Carani did not ask for this file to come on his computer, nor would he have been aware of its existence. [R.131, 494, line 25-495, line 12]. Further, there is no evidence that the file ever had been viewed on the seized computer. [R.131, 495, line 14-20]. Special Agent Skinner stated that he had never been involved in an investigation where child pornography was placed on a computer through a virus or act of another computer user. [R.131, 827, lines 6-14].

Mr. Ellis described that of the deleted files, contained in the .dbb folder, the largest categories were of adult pornography and then music. [R.131, 520, line 3-523, line 7]. Titles suggestive of child pornography made up the third largest category of deleted files. [R.131, 523, line 8-9]. However, he said that the file titles do not always correspond with the content of the files can no longer be determined. [R.131, 523, line 19-524, line 4]. Mr. Ellis tested to determine if the .dbb folder was working properly and determined that it was not, as the "My Shared Folder" had different content then the .dbb folder when they should be

identical. [R.131, 542, line 9-527, line 18]. Special Agent Skinner testified that there was no flaw as he was able to find "a random sampling" of the files and was able to locate them in both locations using a program called Kazaalyzer. [R.131, 815, line 23-820, line 25].

Mr. Ellis also tested Kazaa Lite to search for adult pornography. [R.131, 536, line 9-539, line 5]. He described finding files with child pornography titles, including specific references to 13- and 14-year olds, when he attempted to search for adult pornography. [R.131, 539, line 6-541, line 1]. He concluded that a user searching for adult pornography would obtain results that include child pornography. [R.131, 542, line 22-543, line 5]. Mr. Ellis also opined that the computer's usage suggested that multiple files were downloaded at the same time after a search. [R.131, 612, line 1-613, line 14; 614, line 12-616, line 9; 634; line 18-636, line 18]. Special Agent Skinner testified on re-direct that "files were downloaded in groups of five or six" and that "the child porn seemed to be in a group." [R.131, 821, lines 5-16; 824, lines 10-19]. However, this conclusion was based upon sorting files based upon a review of the time stamps from when the files were "last written," meaning when the download was completed, not based on an analysis of when the downloads began. [R.131, 839, lines 6-16]. Viewing the last written date provides no information as to when the files began to download since files take different amounts of time to download completely and therefore the last written date provides no indication when the files were created. [R.131, 853, line 24-855, line 8].

The trial judge noted that "[t]his court has never tried a child pornography case, nor, as far as we know, have any such cases been tried in this district." [R.60]. During the jury deliberations, the following question was posed to the Court: "Does downloading, watching & deleting constitute possession?" [R.70]. The judge responded, over Mr. Carani's objection [R.136, 16, lines 8-10; 19, lines 4-7; 22, line 24-23, line 5;25, lines 2-3] that:

> "The answer to this question depends upon whether, at the time he downloaded material, the defendant knew or strongly suspected that it was child pornography and downloaded it anyway. If you find beyond a reasonable doubt that he did, then the answer to your question is 'yes.' If you have a reasonable doubt as to whether the defendant knew or strongly suspected that the material was child pornography at the time he downloaded it, then the answer to your question is 'no.' [R.75]."

At sentencing, the government sought an increase in the offense level for "distribution," under U.S.S.G. § 2G2.2(b)(3)(B), as well as other enhancements to the applicable guideline range. [R.100-1]. In support of the requirement that distribution be for "the receipt, or expectation of receipt, of a thing of value," the government stated that: "Thus, but for Carani's willingness to make his files, including his child pornography videos, available to others, he would not have had access to the vast library of materials made available by the other Kazaa users." [R.100-1]. The government also described Carani's computer activity as "active trading" of contraband pornography. [R.100-1].

ARGUMENT

I. PETITIONER'S DECISION TO PROCEED TO TRIAL WAS NOT KNOWINGLY AND VOLUNTARILY MADE, DUE TO INEFFECTIVE ASSISTANCE OF COUNSEL.

The duty of defense counsel is paramount when a criminal defendant has to decide whether or not to waive a constitutional right, such as the right to trial. Because the decision whether or not to plead guilty ultimately rests with the client, counsel must ensure that the client's decision is as informed as possible. See Jones v. Barnes, 463 U.S. 745, 751 (1983) ("the accused has the ultimate authority to make certain fundamental decisions regarding the case, such as whether to plead guilty, waive a jury, testify in his or her behalf, or take an appeal."). See also Wainwright v. Sykes, 433 U.S. 72, 93 n. 1 (1977)(Burger, C.J., concurring) ("[o]nly such basic decisions such as whether to plead guilty, waive a jury, or testify in one's own behalf are ultimately for the accused to make."). Failing to even consider, let alone notify the accused of, a factor that could prevent the accused from making an informed decision as to any of these choices, is not within the wide range of professional norms for competent counsel. That is the case here.

Here, Mr. Carani's counsel never discussed the risks and potential benefits of proceeding to trial versus accepting the government's proposed plea agreement. Rather, counsel merely informed Mr. Carani that the government had offered him a plea agreement, but that Mr. Carani should not take it because counsel believed that Mr. Carani would be acquitted at trial. Notably,

counsel never discussed with, or informed Mr. Carani of the potential differences in his sentence if he was convicted following a trial versus pleading guilty. And critically, counsel never informed Mr. Carani that his handwritten statement dated "2/11/05" constituted an admission of guilt at least for Count One (knowing possession of child pornography), which was the one count Mr. Carani was convicted of. [Exhibit 4].

More specifically, counsel never explained to Mr. Carani that if he pled guilty he would receive a 3-level reduction for acceptance of responsibility. Further, counsel failed to inform Mr. Carani that by proceeding to trial and testifying, he was subjecting himself to a 2-level enhancement for obstruction of justice.

As discussed during Mr. Carani's sentencing hearing, his guideline level was 168-210 months following his trial. [Sent. Tr. at 62]. However, because of the statutory maximum, the government requested a sentence of 120 months. [Sent. Tr. at 62-68]. While the Court did depart downward from the 120-month advisory guideline, it must be pointed out that the Court also made clear that "[a]side from the...obstruction of justice in the commission of perjury,...I believe that a reasonable sentence in this case, all things considered, would be five years, or 60 months...." [Sent. Tr. at 89]. However, because of the obstruction of justice enhancement based on Mr. Carani's trial testimony, the Court sentenced him to a 72-month term of imprisonment. [Sent. Tr. at 91]. Of course, had Mr. Carani accepted the government's proposed plea, Mr. Carani's sentence would be even much less than the 60-months the Court concluded was reasonable, because Mr. Carani would have

been granted a further reduction for acceptance of responsibility.

Critically here, Mr. Carani's written statement dated "2/11/05" amounted to a concession of guilt as to Count One. A fact that is clearly sustained by the jury's verdict of guilt as to that count only. A fact, however, that counsel never explained to Mr. Carani. Had counsel informed Mr. Carani of that fact, and explained to him the potential differences in his sentence between pleading guilty and being found guilty following trial, Mr. Carani would have accepted the government's proposed plea agreement.[1] Alternatively, Mr. Carani would have entered a blind plea to the 3-Count Indictment.

Notably, the Seventh Circuit Court of Appeals has made clear that "[a] reasonably competent attorney will attempt to learn all the facts of the case, make an estimate of the likely sentence, and communicate the result of that analysis before allowing the client to plead guilty." Julian v. Bartley, 495 F.3d 487, 495 (7th Cir. 2007). That same principle applies to an "attorney's incompetence resulting in the defendant's **rejection** of a plea agreement proposal." Paters v. United States, 159 F.3d 1043, 1046 (7th Cir. 1998). (emphasis in original).

As demonstrated previously, it was ultimately Mr. Carani's decision whether to plead guilty or proceed to trial, not his attorney's. Thus, counsel's failure to allow Mr. Carani to make that decision, and to properly advise him in that decision-making

[1] Because counsel never discussed the specifics of the government's plea offer with Mr. Carani, he does not know the exact terms of the proposed plea agreement.

process, cannot be excused as strategic or tactical. As such, counsel's performance cannot be deemed reasonably competent.

In order to demonstrate prejudice from counsel's deficient performance, Mr. Carani "must show (1) through objective evidence that (2) there is a reasonable probability that, but for counsel's inadequate performance, he would have accepted the government's offer." Paters, 159 F.3d at 1047. Like the petitioner in Paters, supra, Mr. Carani "has certainly met the second prong of that test," because "[h]e has **alleged** a reasonable probability that but for counsel's inadequate performance, he would have accepted the government's offer." Id. at 1047 (emphasis in original). [See Exhibit 5 - affidavit of Mr. Carani].

Accordingly, Mr. Carani's sentence should be vacated and he allowed to either accept the government's proposed plea agreement, or enter a blind plea. Alternatively, an evidentiary hearing is required in this matter because Mr. Carani has alleged facts which, if proven, would entitle him to relief. Paters, 159 F.3d at 1049; Daniels v. United States, 54 F.3d 290.

II. PETITIONER WAS DENIED HIS SIXTH AMENDMENT RIGHT TO EFFECTIVE ASSISTANCE OF COUNSEL, DUE TO COUNSEL'S FAILURE TO INVESTIGATE AND PRESENT EVIDENCE MATERIAL TO THE DETERMINATION OF GUILT.[2]

Mr. Carani was charged in the superseding indictment returned by the grand jury, with one count of knowingly possessing a computer

---

[2]Mr. Carani's "repeated declarations of innocence do not prove...that he would not have accepted a guilty plea." Griffin v. United States, 330 F.3d 733, 738 (6th Cir. 2003)[citing North

that contained video images of child pornography (Count One), and two counts of knowing receipt of child pornography (Counts Two and Three). As the Court is well aware, Mr. Carani was convicted on Count One only, a violation of 18 U.S.C. § 2252A(a)(5)(B). And that conviction was obtained only after the Court gave a clarifying instruction to the jury that it could find Mr. Carani guilty if it found that "the defendant knew or strongly suspected that it was child pornography..." that he was downloading. [R.75].[3] Thus, it cannot be disputed that this conviction was a close call. As such, counsel's failure to present evidence, that would have called into question Mr. Carani's alleged knowledge of child pornography images on his computer, is not within the wide range of competence for defense attorneys and, in fact, amounts to seriously egregious conduct.

In November of 2006, a report was published by the United States Patent and Trademark Office ("USPTO"), entitled "Filesharing Programs and Technological Features to Induce Users to Share." This report illustrated how five (5) pupular filesharing programs have "repeatedly deployed features [in their programs] that had a

---

Carolina v. Alford, 400 U.S. 25, 33 (1970)("reasons other than the fact that he is guilty may induce a defendant to so plead...and he must be permitted to judge for himself in this respect.")]. Likewise, the fact that Mr. Carani asserts that he would have entered a guilty plea but for counsel's errors, does not negate his ineffective assistance of counsel claims regarding counsel's performance pretrial, during trial, at sentencing, and on appeal.

[3]The "strongly suspected" jury instruction is addressed in Grounds III and IV herein.

known propensity to trick users into uploading infringing files inadvertently." [Report, at page 1]. Notably, the program involved in this case, i.e., Kazaa, was one of these five programs. The Report identified five such features of these programs as follows:

> "**Redistribution features:** All five programs analyzed have deployed a feature that will, by default, cause users of the program to upload (or 'share') all files that they download. These features create a counter-intuitive link between downloading files for personal use and distributing files to strangers, and they have often been implemented in ways that could make their effects less obvious to new users. Since 2003, lawsuits against users of filesharing programs have made it more important for users to understand the effects of redistribution features. During this period, some programs tended to disclose less information about their redistribution features.
>
> **Share-folder features:** All five of the programs analyzed have developed a feature that lets users store downloaded files in a folder other than the specially created folder that stores downloaded files by default-but does so through an interface that does not warn users that all files stored in the selected folder will be shared. In most cases, the sharing caused by this will be recursive: The program will share not only the files stored in the folder selected to store downloaded files, but also all files stored in any of its subfolders.
>
> **Search-wizard features:** At least three of the programs analyzed have deployed a feature that will search users' hard drives and 'recommend' that users share folders that contain certain 'triggering' file types, which usually include document files, audio files, audiovisual

files, and image files. Some search-wizard features activate automatically; others require the user to trigger them. Some are activated during a program's installation-and-setup process; others are an option that a user can activate after the program is installed and running. Some will select identified folders for sharing; others 'recommend,' but do not select, identified folders for sharing. All search-wizard features discussed will cause recursive sharing of identified or selected folders.

Partial-uninstall features: At least four of the programs analyzed have deployed partial-uninstall features: If users uninstall one of these programs from their computers, the process will leave behind a file that will cause any subsequent installation of any version of the same program to share all folders shared by the 'uninstalled' copy of the program. Whenever a computer is used by more than one person, this feature ensures that users cannot know which files and folders these programs will share by default.

Coerced-sharing features: Four of the programs analyzed have deployed features that make it far more difficult for users to disable sharing of the folder used to store downloaded files. This folder may be the default download folder created by the filesharing program or an existing folder selected to store downloaded files through a share-folder feature. In each case, the feature can provide misleading feedback indicating - incorrectly - that the user has disabled sharing of the download folder. But in each case, an obscure mechanism appears to allow sophisticated users to avoid the coerced-sharing feature and stop sharing the download folder."

[Exhibit 6].

This report demonstrates that the Kazaa program involved in this case has been causing inadvertent sharing since its inception. In other words, the report makes clear that Mr. Carani's Kazaa program was capable of both receiving (downloading) and sending (uploading) files that he had absolutely no knowledge of. While this report was not issued until 2006, "**[p]ublished** research identified these features as causes of inadvertent sharing by **mid-2002.**" [Exhibit 6, at page 2]. As such, the information in this report was undoubtably available to Mr. Carani's attorney to present during this trial.

To establish ineffective assistance of counsel, Mr. Carani must "show that [his] counsel's performance was deficient, and that the deficiency prejudiced [his] defense." Wiggins v. Smith, 539 U.S. 510, 521 (2003). According to the Supreme Court, "The proper measure of attorney performance remains simply reasonableness under prevailing professional norms." Strickland v. Washington, 466 U.S. 668 (1984). Notably, a "counsel has a duty to make reasonable investigations or to make a reasonable decision that makes particular investigations unnecessary." Id. at 466 U.S. 691. Here, there can be no strategic or tactical reason that could excuse counsel's failure to investigate the Kazaa program that was on Mr. Carani's computer, especially when there was "[p]ublished research" available "by mid-2002." [Exhibit 6, at 2]. Critically, had Mr. Carani's counsel investigated this program and presented this "[p]ublished research" during this trial, there is certainly a reasonable probability that the jury would have also acquitted Mr. Carani of Count One. Strickland, 466 U.S.

at 694 (holding that a defendant is prejudiced by counsel's deficient performance when "there is a reasonable probability that but for counsel's unprofessional errors, the result of the proceeding would have been different. A reasonable probability is a probability sufficient to undermine confidence in the outcome."). This is clearly such a case.

Accordingly, Mr. Carani's conviction and sentence should be set aside and vacated, and Mr. Carani granted a new trial. Alternatively, counsel should be appointed and this matter scheduled for an evidentiary hearing.

III. PETITIONER WAS DENIED HIS SIXTH AMENDMENT RIGHT TO EFFECTIVE ASSISTANCE OF COUNSEL, DUE TO COUNSEL'S FAILURE TO ARGUE AT THE DISTRICT LEVEL AND ON APPEAL THAT THE COURT CONSTRUCTIVELY AMENDED THE INDICTMENT.

To be found guilty of a violation of 18 U.S.C. § 2252A(a)(5)(B), the government must prove beyond a reasonable doubt that the defendant "**knowingly** possesse[d] any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography...." Id. Here, Mr. Carani was charged with one count of possession under § 2252A(a)(5)(B), and two counts of receipt under § 2252A(a)(2)(A). The jury found Mr. Carani not guilty of one count of receipt and was unable to return a verdict on the other count. With regard to the possession count, the jury posed the following question to the Court: "Does downloading, watching and deleting constitute possession?" Critically, and over Mr. Carani's objections, the Court responded:

> "The answer to this question depends upon whether, at the time he downloaded material, the defendant knew **or strongly suspected** that it was child pornography...." (emphasis added). [R.75].

Mr. Carani respectfully submits that this supplemental jury instruction amounted to no less than a constructive amendment of the indictment in at least one of two ways.

First, the essential elements of § 2252A(a)(5)(B) are knowing possession of some type of a "container" that holds images of child pornography. See United States v. Hall, 142 F.3d 988, 998 (7th Cir. 1998)[holding that a computer and its files were containers for the purposes of § 2252(a)]. As such, the district court's supplemental jury instruction left out the "container" requirement constructively amended Count One of this Indictment.

Second, the district court's instruction to the jury that it could find the essential element of "knowledge" by finding that Mr. Carani "strongly suspected," also constitutes an impermissable constructive amendment of Count One. In United States v. Myers, 355 F.3d 1040, 1042 (7th Cir. 2004), the Seventh Circuit discussed the essential element of knowledge:

> "The Supreme Court has held that the prohibition on receipt of child pornography in § 2252(a)(2) includes a scienter requirement, and therefore encompasses **only** situations in which the defendant **knows** that the material he is receiving depicts minors engaged in sexually explicit conduct. United States v. X-Citement Video, Inc., 513 U.S. 64, 78, 115 S.Ct. 464, 130 L.Ed.2d 372 (1994). Accordingly, a person **who seeks out only adult pornography, but without his knowledge is sent a mix of adult and child pornography**, will not have violated that statutory

> provision. That same person, however, could be in violation of the possession provision of § 2252(a)(4)(B) **if** he or she **decides to retain** that material, thereby knowingly possessing it." (emphasis added).

Critically, the supplemental jury instruction completely changed the essential elements of the "possession" count the jury inquired about, to elements constituting "receipt" of child pornography. Myers, supra.

A constructive amendment of an indictment can occur "either through the evidence or through the jury instruction." United States v. Jefferson, 334 F.3d 670, 673 (7th Cir. 2003). The Court in Jefferson defined a constructive amendment as follows:

> "[A] constructive amendment occurs where proof at trial goes beyond the parameters of the indictment in that it establishes offenses **different from or in addition to** those charged by the grand jury. Such error...which in a jury trial can also be **generated or exacerbated by faulty instructions**, violates the Fifth Amendment since the Grand Jury Clause limits the available basis for conviction to those contained in the indictment." [quoting United States v. Pigee, 197 F.3d 879, 886 (7th Cir. 1999)(emphasis added)].

Critically, when such an amendment occurs, the error is structural and not subject to harmless error analysis, thus, requires per se reversal of the conviction. United States v. McAnderson, 914 F.2d 934, 944 (7th Cir. 1990).

Accordingly, counsel's failure to challenge this constructive amendment at the district level, and/or to raise the issue in the direct appeal of this case, constitutes ineffective assistance of counsel. See Lucas v. O'Dea, 179 F.3d 412, 419 (6th Cir. 1999);

Gray v. Lynn, 6 F.3d 265, 270-71 (5th Cir. 1993). As such, Mr. Carani's conviction and sentence should be set aside and vacated. Alternatively, an evidentiary hearing is mandated by statute and controlling precedent.

IV. PETITIONER WAS DENIED HIS SIXTH AMENDMENT RIGHT TO EFFECTIVE ASSISTANCE OF COUNSEL, DUE TO COUNSEL'S FAILURE TO ARGUE AT THE DISTRICT LEVEL AND ON APPEAL, THAT THE SUPPLEMENTAL JURY INSTRUCTION BY THE COURT RESULTED IN AN IMPERMISSIBLE GENERAL VERDICT THAT IS NOT SUBJECT TO HARMLESS ERROR REVIEW.

In affirming the district court's supplemental jury instruction, the Seventh Circuit noted that it was an incorrect statement of law. However, the Seventh Circuit nonetheless concluded that Mr. Carani was not prejudiced by the instruction and, in fact, benefited from the instruction. [Exhibit 1, at 12-13]. Simply put, there is no authority known that could change the government's burden to prove Mr. Carani "knowingly" possessed child pornography to a burden of "strongly suspected." See United States v. Turcotle, 405 F.3d 515, 528-29 (7th Cir. 2005)(discussing the scienter requirement of "knowledge"); United States v. X-Citement Video, Inc., 513 U.S. 64 (1994).

The landmark opinion in Morissette v. United States, 342 U.S. 246, 96 L.Ed. 288, 72 S.Ct. 240 (1952), discussed the common law history of mens rea as applied to the elements of the federal embezzlement statute. That statute reads: "Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States...

[s]hall be fined." 18 U.S.C. § 641 [18 U.S.C.S. § 641], cited in Morissette, 342 U.S. at 248, n.2, 96 L.Ed. 288, 72 S.Ct. 240. Perhaps even more obvious in the statute here, the essential element "knowing" in its isolated position requires that the defendant intentionally assumed dominion over the property. But the Seventh Circuit used the background presumption of evil intent to conclude that the term "knowingly" would also be proven if the jury "strongly suspected" that the downloaded material was child pornography, a conclusion that did not benefit Mr. Carani. See also United States v. United States Gypsum Co., 438 U.S. 422, 438, 57 L.Ed.2d 854, 98 S.Ct. 2864 (1978)("[F]ar more than the simple omission of the appropriate phrase from the statutory definition is necessary to justify dispensing with an intent requirement").

Liparota v. United States, 471 U.S. 419, 85 L.Ed.2d 434, 105 S.Ct. 2084 (1985), posed a challenge to a federal statute prohibiting certain actions with respect to food stamps. The statute's use of "knowingly" could be read only to modify "uses, transfers, acquires, alters, or possesses" or it could be read also to modify "in any manner not authorized by [the statute]." Noting that neither interpretation posed constitutional problems, id., at 424, n.6, 85 L.Ed.2d 434, 105 S.Ct. 2084, the Court held the scienter requirement applied to both elements by invoking the background principle set forth in Morissette. In addition, the Court was concerned with the broader reading which would "criminalize a broad range of apparently innocent conduct." 471 U.S. at 426, 85 L.Ed.2d 434, 105 S.Ct. 2084. Imposing criminal liability on an unwitting food stamp recipient who purchased groceries at a store that

inflated its prices to such purchasers struck the Court as beyond the intended reach of the statute.

The same analysis drove the recent conclusion in Staples v. United States, 511 U.S. ___, 128 L.Ed.2d 608, 114 S.Ct. 1973 1994, that to be criminally liable a defendant must know that his weapon possessed automatic firing capability so as to make it a machine gun as defined by the National Firearms Act.

Morissette, reinforced by Staples, instructs that the presumption in favor of a scienter requirement should apply to each of the statutory elements which criminalize otherwise innocent conduct.

Both federal and State Courts have held, under a variety of rationales, that the giving of an instruction similar to that challenged here is fatal to the validity of a criminal conviction for several reasons.

First, a reasonable jury could well have interpreted the presumption as "conclusive," that is, not technically as a presumption at all, but rather as an irrebuttable direction by the Court to find intent once convinced of the facts triggering the presumption. Alternatively, the jury may have interpreted the instruction as a direction to find intent upon proof of the defendant's voluntary actions (and their "ordinary" consequences), unless the defendant proved the contrary by some quantum of proof which may well have been considerably greater than "some" evidence - thus effectively shifting the burden of persuasion on the element of intent.

In Morissette, supra, the Supreme Court made clear:

"It follows that the trial court may not withdraw or

> prejudge the issue by instruction that the law raises a presumption of intent from an act. It often is tempting to cast in terms of a 'presumption' a conclusion which a court thinks probable from given facts.... [B]ut [w]e think presumptive intent has no place in this case. A conclusive presumption which testimony could not overthrow would effectively eliminate intent as an ingredient of the offense. A presumption which would permit but not require the jury to assume intent from an isolated fact would prejudge a conclusion which the jury should reach of its own volition. A presumption which would permit the jury to make an assumption which all the evidence considered together does not logically establish would give to a proven fact an artificial and fictional effect. In either case, **this presumption would conflict with the overriding presumption of innocence with which the law endows the accused and which extends to every element of the crime."** Id. at 274-275, 96 L.Ed. 288, 72 S.Ct. 240. (emphasis added; footnote omitted).

"[I]t has long been settled that when a case is submitted to the jury on alternative theories the unconstitutionality of any of the theories requires that the conviction be set aside." Sandstrom v. Montana, 442 U.S. 510, 526, 99 S.Ct. 2450, 61 L.Ed.2d 39 (1979) (citation, alternation, and internal quotation marks omitted). See also Zant v. Stephens, 463 U.S. 862, 881, 103 S.Ct. 2733, 77 L.Ed. 2d 235 (1983)("[A] general verdict must be set aside if the jury was instructed that it could rely on any of two or more independent grounds, and one of those grounds is insufficient, because the verdict may have rested exclusively on the insufficient ground."); Yates v. United States, 345 U.S. 298, 312, 77 S.Ct. 1064, 1 L.Ed.2d

1356 (1957)("[T]he proper rule to be applied is that which requires a verdict to be set aside in cases where the verdict is supportable on one ground, but not on another, and it is impossible to tell which ground the jury selected"), overruled on other grounds, Burks v. United States, 437 U.S. 1, 98 S.Ct. 2141, 57 L.Ed.2d 1 (1978); Stromberg v. California, 283 U.S. 359, 368, 51 S.Ct. 532, 75 L.Ed. 1117 (1931)("[I]f any of the clauses [of the statute] in question is invalid under the Federal Constitution, the conviction cannot be upheld.").

This line of cases, originating with Stromberg, makes clear that "when a jury delivers a general verdict that may rest either on a legally valid or legally invalid ground[,]...the verdict may not stand when there is no way to determine its basis." Keating v. Hood, 191 F.3d 1053, 1062 (9th Cir. 1999). See also United States v. Fulbright, 105 F.3d 443, 451 (9th Cir.), cert. denied, 520 U.S. 1236, 117 S.Ct. 1836, 137 L.Ed.2d 1041 (1997)("Where a jury returns a general verdict that is potentially based on a theory that was legally impermissible or unconstitutional, the conviction cannot be sustained.")(emphasis in original).

This is clearly such a case. The Court of Appeals for the Seventh Circuit agreed that the "strongly suspected" jury instruction was erroneous. [Exhibit 1, at page 11-13]. However, when the district court instructed the jury that it could convict Mr. Carani if it believed he **either** "knew or **strongly suspected,**" the district court permitted the jury to return a general verdict that is potentially based on a theory that was legally impermissible or unconstitutional." Fulbright, 105 F.3d at 451. Critically, in such

cases, harmless error analysis does not apply.

As such, Mr. Carani's counsels were constitutionally deficient for failing to make this argument at the district level and on appeal, especially in light of the well-known case law pertaining to this issue. But for counsels' failures to raise this argument, there is a reasonable probability that Mr. Carani would have also been acquitted on Count One, and/or the Seventh Circuit would have reversed this conviction.

Accordingly, Mr. Carani is entitled to have his conviction and sentence set aside and vacated, and a new trial granted. Alternatively, an evidentiary hearing is required in this matter.

V. PETITIONER WAS DENIED HIS SIXTH AMENDMENT RIGHT TO EFFECTIVE ASSISTANCE OF COUNSEL, DUE TO COUNSEL'S FAILURE TO INFORM PETITIONER OF THE RISKS OF TESTIFYING, AND FOR FAILING TO INFORM PETITIONER THAT THE DECISION WHETHER OR NOT TO TESTIFY BELONGED TO PETITIONER.

A criminal defendant's right to testify is "a fundamental constitutional right." Rock v. Arkansas, 483 U.S. 44, 53 (1987). Established doctrine has it that some rights are so important that only the defendant may make the decision whether to exercise those rights or waive them. "The right to trial by jury is in this category: so is the right to testify in one's own defense." United States v. Babul, 476 F.3d 498, 500 (7th Cir. 2007). In fact, this Circuit has made clear that the right to choose whether or not to testify is "[e]ven more fundamental to a personal defense than the right to self-representation." Ward v. Sternes, 334 F.3d 696, 705 (7th Cir. 2005).

Here, Mr. Carani was never given that choice. In fact, Mr. Carani was never informed that it was solely his decision whether or not to testify during this trial. Rather, counsel merely told Mr. Carani that he was going to testify so that the jury could hear his defense. Moreover, Mr. Carani was never told that his testimony could be used to enhance his sentence if he was found guilty.

While it is certainly true that a defense attorney's strategic decisions are not normally subject to a reasonably competent analysis under Strickland, such defense is not applicable when the deficient performance involves a defendant's fundamental rights that is not part of the attorney's strategic decisions. In other words, some rights - such as Mr. Carani's right to testify - are fundamental constitutional rights, thus, an attorney cannot waive or exercise those rights because that decision belongs solely to the defendant.

As such, a reasonably competent attorney would never make such a decision for his or her client. In addition, a reasonably competent attorney would inform the defendant that such a decision was solely the defendant's. Moreover, a reasonably competent attorney would advise that defendant as to the possible risks of testifying. Because Mr. Carani's attorney failed to perform any of these basic duties, counsel was constitutionally deficient.

Critically, Mr. Carani was prejudiced by this deficient performance. Mr. Carani's sentence was increased twelve (12) months solely because of his trial testimony. [Sent. Tr. 89-90]. Had Mr. Carani been informed that he could receive such an enhancement, and

had he been informed that it was his choice whether or not to testify, he would not have testified. And, had Mr. Carani not testified, his sentence would have been "five years, or 60 months," instead of the 72 months imposed. [Sent. Tr. at 89]. See Glover v. United States, 121 S.Ct. 696 (2001)(holding that a § 2255 petitioner demonstrates prejudice under Strickland merely by showing that defense counsel's error(s) resulted in even one more day in prison).

Accordingly, Mr. Carani's sentence should be corrected to reflect a sentence without the obstruction of justice enhancement imposed for his trial testimony, i.e., a sentence of "five years, or 60 months." Id. Alternatively, an evidentiary hearing is mandated by Circuit precedent because "a determination of credibility cannot be made on the basis of an affidavit." Daniels, 54 F.3d at 295 [quoting Castillo v. United States, 34 F.3d 443, 445 (7th Cir. 1994)].

VI. PETITIONER WAS DENIED HIS SIXTH AMENDMENT RIGHT TO EFFECTIVE ASSISTANCE OF COUNSEL, DUE TO COUNSEL'S FAILURE TO PRESENT EVIDENCE AND ARGUMENT AT SENTENCING AND ON APPEAL THAT WOULD HAVE SUSTAINED PETITIONER'S OBJECTION TO THE 2-LEVEL ENHANCEMENT FOR DISTRIBUTION.

During this sentencing hearing, Mr. Carani's counsel did object to and challenge the 2-level enhancement under § 2G2.2(b)(3)(F) for distribution of child pornography. In fact, Mr. Carani's counsel challenged this enhancement on appeal. However, counsels failed to present evidence and argument that would have sustained that objection at the district level, and/or vacated that

enhancement on appeal.

1. The failure to present evidence:

First, the evidence presented at trial by the government did not show that Mr. Carani distributed child pornography knowingly. In fact, government witness Jennifer Sapper, a special agent with the Department of Homeland Security, Immigration and Customs Enforcement ("ICE") testified otherwise. Specifically, the following colloquy occurred:

Q: He's not been charged with distributing child pornography, though has he?

Agent Sapper: No, he has not.

Q: You have **no information** that he was trying to distribute child pornography...?

Agent Sapper: No, I do not.

Critically, however, counsel failed to bring this evidence to the attention of the Court at sentencing.

Notably, and as previously presented in Ground II herein, a report was published by the United States Patent and Trademark Office ("USPTO") in 2006, entitled "Filesharing Programs And Technological Features To Induce Users To Share." [Exhibit 6]. This report illustrated how five (5) popular filesharing programs have repeatedly deployed featrues [in their programs] that had a known propensity to trick users into uploading infringing files inadvertently." [Exhibit 6, at page 1]. As also demonstrated, the program involved in this case, i.e., Kazaa, was one of these five programs. Finally, Mr. Carani demonstrated through this report

that "[p]ublished research identified these as causes of inadvertent sharing by mid-2002." [Exhibit 6, at page 2].

As such, there is no reasonable tactical or strategic excuse that could justify counsel's failure to present this evidence and make this argument during sentencing, since it has clearly been available since "mid-2002." Id. Had counsel done so, there is a reasonable probability that the enhancement would not have been applied.

Accordingly, Mr. Carani is entitled to a correction of sentence to reflect a sentence without this 2-level enhancement. Otherwise, an evidentiary hearing should be held.

2. The failure to argue that the enhancement constituted impermissable double counting:

As stated above, the Court enhanced Mr. Carani's sentence 2-levels under § 2G2.2(b)(3)(F) for distribution. In addition, the Court also enhanced Mr. Carani's sentence 2-levels under subsection (b)(6) for "distribution of the material..." through "the use of a computer." Id. [See also Sent. Tr. at 39-40]. Mr. Carani respectfully submits that both enhancements constitute impermissible double counting, simply because both enhancements are imposed for the "distribution" of child pornography. Id.

In light of the long-standing prohibition against duplicative punishments for conduct amounting to essentially the same harm, counsels' failure to raise this argument at the district level and on appeal was constitutionally deficient. Had counsels raised this argument, there is a reasonable probability that one of these 2-

level enhancements would not have been imposed.

As such, Mr. Carani's sentence should be corrected accordingly. Alternatively, an evidentiary hearing should be held in this matter.

VII. PETITIONER WAS DENIED HIS SIXTH AMENDMENT RIGHT TO EFFECTIVE ASSISTANCE OF COUNSEL, DUE TO COUNSEL'S FAILURE TO ARGUE AT SENTENCING AND ON APPEAL THAT PETITIONER'S SENTENCE WAS IMPOSED IN VIOLATION OF HIS FIFTH AND SIXTH AMENDMENT RIGHTS.

During sentencing, the Court imposed several enhancements on Mr. Carani based on alleged conduct that was not included in the indictment, and that the jury had acquitted Mr. Carani of. For example, the Court applied a 2-level enhancement for distribution, and another 5-level enhancement for receipt of over 600 images. Critically, the government's own witness - Special Agent Jennifer Sapper - testified that there was no information or evidence that Mr. Carani had been trying to distribute child pornography. [R: 131, 115; lines 19-24]. Further, although Mr. Carani was charged with two counts of receiving child pornography, the jury acquitted him of one count and was unable to return a verdict on the other count. Thus, for the district court to make determinations completely contrary to the evidence is clearly erroneous and, in fact, a violation of Mr. Carani's fundamental constitutional rights.

Specifically, this enhancement amounts to no less than a violation of Mr. Carani's Fifth Amendment right to be punished only on findings proven beyond a reasonable doubt, and his Sixth Amendment right to a jury determination of any fact that increases his

sentence, as clearly set out in United States v. Booker, 543 U.S. 220 (2005) and United States v. Rita, No. 06-5754. Specifically, these enhancements were the sole result of the district court's judge's factual determination. A finding that was neither determined by the jury or admitted to by Mr. Carani.

As the Supreme Court's decisions instruct, the Federal Constitution's jury-trial guarantee proscribes a sentencing scheme that allows a judge to impose a sentence above the statutory maximum based on a fact, other than a prior conviction, not found by a jury or admitted by the defendant. Apprendi v. New Jersey, 530 U.S. 466 (2000); Ring v. Arizona, 536 U.S. 584 (2002); Blakely v. Washington, 542 U.S. 296 (2004); United States v. Booker, 543 U.S. 220 (2005). "[T]he relevant 'statutory maximum,'" the Court has clarified, "is not the maximum sentence a judge may impose after finding additional facts, but the maximum he may impose without any additional findings." Blakely, 542 U.S. at 303-304 (emphasis in original).

As the Supreme Court stated in Blakely:

> "Our precedents make clear...that the 'statutory maximum' for Apprendi purposes is the maximum sentence a judge may impose solely on the basis of the facts reflected in the jury verdict or admitted by the defendant.... In other words, the relevant 'statutory maximum' is not the maximum sentence a judge may impose after finding additional findings. When a judge inflicts punishment that the jury's verdict alone does not allow, the jury has not found all the facts 'which the law makes essential to the punishment,'...and the judge exceeds his proper authority." Id. at 303 (emphasis in original)(quoting 1

J. Bishop, Criminal Procedure § 87, p.55 (2nd ed. 1872)).

In Rita, supra, the Supreme Court did not specifically address the Sixth Amendment's jury protections, because the petitioner's sentence was not determined by judge-found facts. Rather, the sole question before the Court was whether the law permits the Court of Appeals to employ a presumption of reasonableness **review on appeal.** Nonetheless, the Rita Court reiterated the Court's Sixth Amendment jurisprudence:

> "The Sixth Amendment question, the Court has said, is whether the law forbids a judge to increase a defendant's sentence unless the judge finds facts that the jury did not find (and the offender did not concede). Blakely, supra, at 303-304 ('When a judge inflicts punishment that the jury's verdict alone does not allow, the jury has not found all the facts which the law makes essential to the punishment and the judge exceeds his proper authority' (internal quotation marks and and citation omitted)); see Cunningham, supra, at ___, (Slip Op., 10, 11)(discussing Blakely)('The judge could not have sentenced Blakely above the standard range without finding the additional fact of deliberate cruelty,' '[b]ecause the judge in Blakely's case could not have imposed a sentence outside the standard range without finding an additional fact, the top of that range...was the relevant' maximum sentence for Sixth Amendment purposes); Booker, 543 U.S. at 244 ('Any fact (other than a prior conviction) which is necessary to support a sentence exceeding the maximum authorized by the facts established by a plea of guilty or a jury verdict must be admitted by the defendant or proved to a jury beyond a reasonable doubt'); id. at 232 (discussing Blakely)('We rejected the State's argument that the jury verdict was sufficient to authorize a sentence

> within the general 10-year sentence for Class B felonies, noting that under Washington law, the judge was **required** to find additional facts in order to impose the greater 90-month sentence')(emphasis in original))."

Irrespective of the current advisory nature of the Guidelines, the district court's determinations violated Mr. Carani's Fifth and Sixth Amendment rights, and are in direct conflict with Supreme Court precedent, in light of the evidence presented to the contrary at trial and the jury's failure to make such a finding. Recently, the Supreme Court addressed a similar situation in Cunningham v. California, 549 U.S. ___, (2007). In concluding that California's determinate sentencing scheme violated the Petitioner's Sixth Amendment rights, the Court stated:

> "This Court has repeatedly held that, under the Sixth Amendment, any fact that exposes a defendant to a greater potential sentence must be found by a jury, not a judge, and established beyond a reasonable doubt, not merely by a preponderance of the evidence. While this rule is rooted in long standing common-law practice, its explicit statement in our decisions is recent. In Jones v. United States, 526 U.S. 227 (1999), we examined the Sixth Amendment's historical and doctrinal foundations, and recognized that judicial factfinding operating to increase a defendant's otherwise maximum punishment posed a grave constitutional question. Id. at 239-252. Slip opinion, at 8."

Accordingly, counsel's failure to raise this argument at sentencing and on appeal cannot be deemed reasonably competent, especially in light of the plain language of Apprendi, Ring, Blakely, and Booker. Had counsel raised this argument and invoked

Mr. Carani's Fifth and Sixth Amendment rights, there is a reasonable probability that Mr. Carani's sentence would have been less. Glover, supra.

As such, Mr. Carani's sentence should be corrected to reflect an advisory guideline range determined without violating Mr. Carani's Fifth and Sixth Amendment rights. Otherwise, an evidentiary hearing should be scheduled as soon as possible.

VIII. PETITIONER WAS DENIED HIS SIXTH AMENDMENT RIGHT TO EFFECTIVE ASSISTANCE OF COUNSEL, DUE TO COUNSEL'S FAILURE TO PROPERLY CHALLENGE THE 5-LEVEL ENHANCEMENT AT SENTENCING, AND FAILURE TO RAISE THE ISSUE ON DIRECT APPEAL.

During this sentencing, the government argued that a 5-level enhancement was appropriate under § 2G2.2(b)(7)(D) because "there are eight unique child pornography videos," each of which is "considered to be 75 images." [Sent. Tr. at 40-41]. Thus, according to the government, these 8 videos times 75 images per video equaled the 600 or more images required to sustain the 5-level enhancement requested. Id. In response to this assertion, Mr. Carani's counsel disagreed "that Mr. Carani was aware of any but one video... [j]ust to make my record." [Sent. Tr. at 41]. The Court accepted the government's argument and imposed the 5-level increase. [Sent. Tr. at 41].

Shortly thereafter while discussing the proposed enhancement for alleged perjury by Mr. Carani, defense counsel brought up the point that even though Mr. Carani's computer contained several titles indicative of child pornography, "no one knows whether or

not they are." [Sent. Tr. at 43]. In response, the Court turned to AUSA Ruder and asked:

> "Is there testimony that goes beyond the **two or three videos** that were highlighted at trial that the rest of these videos in fact did involve what the titles imply they did?"
>
> [Sent. Tr. at 44 (emphasis added)].

Critically, AUSA Ruder replied:

> "**No.** And the government's position on that, the whole relevance of these titles, Your Honor, was not that-- **is not what was contained in them....**"
>
> [Sent. Tr. at 44 (emphasis added)].

Clearly, if there are only "three videos" that were testified to, and that the government was interested in "what was contained in them," it was entirely circular for the government to have just argued that there were eight (8) videos containing 75 images of child pornography on each. Id. In fact, it was improper and borders on prosecutorial misconduct.

Nonetheless, it was even more egregious for Mr. Carani's counsels to fail to argue that the 5-level enhancement could not be imposed, when there was testimony as to the contents of only 2-3 videos. This is especially true where, as here, the government admitted that "the government's position..." on these videos was "not what was contained in them." Id. In other words, according to the government "if you're downloading a video called little child is molested, it doesn't matter if it contains a clip of the news or a commercial for tuna or whatever it is." [Sent. Tr. at 44]. Simply put, had Mr. Carani's counsels presented this argument

at the district level or on appeal, there is a reasonable probability that the enhancement would not have been imposed.

As such, Mr. Carani's sentence should be corrected to reflect a sentence without this 5-level enhancement. Alternatively, an evidentiary hearing should be scheduled in this case.

IX. PETITIONER WAS DENIED HIS SIXTH AMENDMENT RIGHT TO EFFECTIVE ASSISTANCE OF COUNSEL ON APPEAL, DUE TO COUNSEL'S FAILURE TO RAISE A SUFFICIENCY OF THE EVIDENCE CHALLENGE.

To be found guilty of a violation of 18 U.S.C. § 2252A(a)(5)(B), the government must prove beyond a reasonable doubt that the defendant "**knowingly** possesse[d] any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography...." Id. Here, Mr. Carani was charged with one count of possession under § 2252A(a)(5)(B), and two counts of receipt under § 2252A(a)(2)(A). The jury found Mr. Carani not guilty of one count of receipt and was unable to return a verdict on the other count. With regard to the possession count, the jury posed the following question to the Court: "Does downloading, watching and deleting constitute possession?" Over Mr. Carani's objections, the Court responded:

> "The answer to this question depends upon whether, at the time he downloaded material, the defendant knew **or strongly suspected that it was child pornography...."** (emphasis added). [R.75].

On appeal, Mr. Carani's counsel asserted that the district court's supplemental jury instruction was error. However, counsel failed to argue that the evidence was insufficient to sustain the

conviction for possession of child pornography, Mr. Carani respectfully submits that counsel's failure to do so is especially egregious in light of the facts and circumstances in this case, along with the controlling law on this subject.

Critically, in response to the jury's request for what constitutes "possession," the Court failed to utilize this Circuit's controlling law regarding that definition. For example, in United States v. Myers, 355 F.3d 1040, 1042 (7th Cir. 2004), the Court held that a defendant was innocent of "receiving" child pornography whenever "a person who seeks out only adult pornography, but without his knowledge is sent a mix of adult and child pornography, will not have violated that statutory provision." Id. The Court proceeded to state "[t]hat same person, however, could be in violation of § 2252(a)(4)(B) **if** he or she decides to **retain that material, thereby knowingly possessing it.**" Id. at 1042. (emphasis added). See also § 2252(a)(4)(B) and § 2252(c)(requiring knowing possession, and including an affirmative defense where such material is promptly and in good faith destroyed).

As stated previously, however, the Court failed to instruct the jury that Mr. Carani was guilty of knowing possession only if he "decide[d] to retain that material." Id. Rather, the Court told the jury that "downloading, watching and deleting constitute[d] possession," if Mr. Carani "knew or strongly suspected that it was child pornography [at the time he] downloaded it." [R:75]. Simply put, it is clear that the jury found Mr. Carani guilty of "possession" because he knew or strongly suspected it was child pornography at the time he "received" it. Critically, there is no

indication, thus, it cannot be reasonably inferred, that the jury found Mr. Carani guilty because he knowingly **retained** the material. Myers, supra.[4]

With respect to Kazaa, only after the file has been downloaded and viewed can a user have knowledge that the file contains sexually explicit material and that a minor is a subject of the material. Absent such knowledge, a prosecution for knowing possession of child pornography fails. United States v. X-Citement Video, Inc., 513 U.S. 64 (1994). A defendant may be convicted of unlawful possession of child pornography "only upon a showing that he knew the matter in question contained an unlawful visual depiction." United States v. Lacy, 119 F.3d 742, 747 (9th Cir. 1997), cert. denied, 523 U.S. 1101 (1998); see also United States v. Cedelle, 89 F.3d 181, 185 (4th Cir. 1995).[5]

A number of courts have had occasion to address what constitutes "knowing possession" with respect to computer files. A leading case regarding possession of child pornography is United States v. Tucker, 305 F.3d 1193, 1204 (10th Cir. 2002). Tucker

---

[4]While the supplemental jury instruction was found to be erroneous by the Seventh Circuit Court of Appeals, the Court did not undertake a sufficiency of the evidence analysis because the issue was not raised on appeal.

[5]See also, Ty E. Howard, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files. 19 BERKLEY TECH.L.J. 1227 (2004). In this article, the author notes that, "deletion of a file does not provide a sound, much less sufficient basis on which to find knowing possession." Id.

dealt with files obtained from websites (again where a user is able to see the content of the file before choosing whether to download/save the file). In Tucker, the district court concluded that the defendant's possession was knowing, since he purposefully visited websites containing child pornography knowing that the images would be stored on his computer's hard drive. Id. at 1269.

In Tucker, the record reflected testimony that:

> "Using specialized software, [a forensic computer expert] recovered some 27,000 images stored on Tucker's computer. [The expert] estimated that of the .jpg images which were viewable, ninety to ninety-five percent were child pornography.... [The expert] rejected the suggestion that Tucker had accidentally run across these images, citing Web browser history files which showed that Tucker repeatedly visited the same sites. Through [the expert], the government also presented an email from Tucker to a Website operator asking to be given access to pictures of "naked young girls."

Tucker, 305 F.3d at 1197-1198.

The district court in Tucker concluded that the defendant possessed child pornography within the meaning of 18 U.S.C. § 2252A(a)(5)(B). Thus, the crux of "knowing possession" as construed by the Court in Tucker hinged on the uncontested evidence that the defendant e-mailed a website operator to obtain pictures of "naked young girls."

The Ninth Circuit recently found that it "agree[d] generally with Tucker's analysis" described below and that "the defendant must, at a minimum, know that the unlawful images are stored on a disk or other tangible material in his possession." United States

v. Romm, 455 F.3d 990, 1000 (9th Cir. 2006).

Further, Tucker dealt with the routine deletion of images that were previously viewed by a user on the same websites; in contrast, a Kazaa user does not view an image or video or hear a song until it has been downloaded. Thus, the content of a file is unknown to a Kazaa user until that file is downloaded and accessible.

In United States v. Stulock, 308 F.3d 922, 925 (8th Cir. 2002), the Eighth Circuit found insufficient evidence to sustain a conviction for "knowing possession" of child pornography obtained through websites, despite evidence of accessing files with names associated with child pornography, because after the user viewed the images (which resulted in their being automatically cached on his computer), he took no further action to manipulate the file. Here, when using Kazaa, Mr. Carani accessed files with titles suggestive of child pornography and downloaded the files, which is a prerequisite to viewing the file. If Mr. Carani viewed a contraband file, he took no action to store the files further within his computer; instead, he deleted the files.

Here, the evidence at trial demonstrated that Mr. Carani searched for adult pornography. He never contacted any computer user or website operator in search of contraband pornography. Mr. Carani did not belong to any Yahoo! groups or other groups which dealt with child pornography or a sexual interest in children.

The video file for which Mr. Carani was convicted of "knowingly possessing" was obtained through Kazaa. There was no evidence that this file was located through use of a search designed

to locate files pertaining to illicit pornography. [R.131, 378, line 23-379, line 2]. The government did **not produce any evidence that the file was viewed following it being downloaded.** Absent viewing, Mr. Carani could not have made a conscious choice to **retain** the file. Rather, the situation was akin to having an unopened opaque envelope, the contents of which Mr. Carani did not yet make a choice to retain or discard.

Thus, despite the Court's supplemental jury instruction, the viewing and deletion of a file obtained from Kazaa was insufficient to sustain a conviction for "knowing possession" of child pornography. Much like the contents of the opaque envelope, one cannot knowingly possess a contraband computer file if he is unaware of its content. United States v. X-Citement Video, Inc., 513 U.S. 64, 71-73 (1994); United States v. Lacy, 119 F.3d 742, 747 (9th Cir. 1997); United States v. Cedelle, 89 F.3d 181, 185 (4th Cir. 1996). At best, the government's evidence here showed that, once he viewed a file containing child pornography, Mr. Carani sought to promptly to dispossess it---not to possess it.

The Ninth Circuit summarized the rationale of X-Citement Video that "[d]istribution of sexually explicit material involving minors is not. Unless a distributor knew the performers were underage, the Court reasoned, he would have reasonably expected his conduct to be legal." United States v. Lacy, 119 F.3d 742, 747 (9th Cir. 1997), cert. denied, 523 U.S. 1101 (1998). In the context of peer-to-peer file programs, one cannot be aware of the content of the file until after it is downloaded and viewed. Thus, unlike in the context of internet files, deletion of a file obtained from Kazaa

cannot be a sufficient basis for a determination of "knowing possession." An internet user chooses to obtain a file after observing its content; a Kazaa user has no such opportunity. Thus in downloading a file of unknown content a Kazaa user, like Carani," would have reasonably expected his conduct to be legal." Id.

Accordingly, there is no reasonable or justifiable strategic or tactical excuse for counsel's failure to challenge the sufficiency of the evidence on appeal. Clearly, the jury's verdict was based on an incorrect instruction from the Court. An instruction that was far more appropriate for the "receiving" counts than the "possession" count. Critically, no rational juror would have returned a guilty verdict against Mr. Carani had he or she been properly instructed on the elements of Count One. Myers, supra. See United States v. Hilton, 363 F.3d 58, 63-66 (1st Cir. 2004) (affirming district court's granting of habeas relief based on insufficiency of the evidence); United States v. Sims, 220 F.Supp. 2d 1222, 1228-29 (D.N.M. 2002)(granting judgment of acquittal following trial). As such, there is a reasonable probability that Mr. Carani's conviction would have been vacated on appeal, had counsel raised and properly challenged the sufficiency of the evidence.

Accordingly, Mr. Carani's conviction and sentence should be set aside and vacated, and Mr. Carani granted immediate release. Alternatively, Mr. Carani's sentence should be vacated and reinstated to vindicate his Sixth Amendment right to effective assistance of counsel on his appeal of first right. Otherwise, an evidentiary hearing is required by statute and Circuit precedent.

CONCLUSION

Wherefore, due to the foregoing reasons and law, Petitioner's sentence should be vacated, set aside, or corrected, along with any other fair and just relief this Court deems appropriate. Alternatively, counsel should be appointed and an evidentiary hearing scheduled as soon as practical.

Respectfully Submitted on this, the 1 day of DEC., 2007.

Fabio Carani

Fabio Carani
Reg. No. 21827-424
FCI Ashland
P.O. Box 6001
Ashland, Kentucky 41105

E X H I B I T 1

In the
United States Court of Appeals
For the Seventh Circuit

No. 06-2007

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

FABIO CARANI,

Defendant-Appellant.

Appeal from the United States District Court
for the Northern District of Illinois, Eastern Division.
No. 05 CR 150 John F. Grady, *Judge.*

ARGUED APRIL 9, 2007 DECIDED JULY 6, 2007

Before EASTERBROOK, *Chief Judge*, and KANNE and WILLIAMS, *Circuit Judges.*

KANNE, *Circuit Judge.* Fabio Carani was charged with one count of possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), and two counts of knowingly receiving child pornography in the form of certain computer files in violation of 18 U.S.C. § 2252A(a)(2)(A). A jury found Carani guilty of possession, but returned a verdict of not guilty as to one of the receipt counts, and was unable to reach a unanimous decision as to the other receipt count. The district court sentenced Carani to seventy-two months' imprisonment. Carani appeals both his conviction and sentence. Finding no error, we affirm.

I. BACKGROUND

Carani is an Italian immigrant who moved to the United States in 1972. He, along with his wife Natza, owned a computer. On this computer, Carani used a program called Kazaa Lite ("Kazaa").

Kazaa is a peer-to-peer file sharing program through which users may download files (music, videos, text, etc.) from the computers of other Kazaa users. Users search for files using search terms as they would in a web browser. Kazaa returns a list of available files that fit the users' search criteria. Users may gain more information about the files by hovering over the file name with the computer cursor. These files are located on the computers of other Kazaa users, not on the Internet at large. The purpose of Kazaa is to allow its users to share such files with each other. When files are completely downloaded or shared through Kazaa, a record of that activity is logged on the user's computer in a database located in what we will call the ".db folder."

Files that are downloaded using Kazaa are placed, by default, in the user's "My Shared Folder." If a user does not wish to allow other users to access his files, he may change his Kazaa settings so that he may download files from others' computers, but they may not download files from his computer. In order to encourage users to share their files, Kazaa employs a participation level system. Participation levels range from 0 to 1,000, and increase with the number of files the user shares. When multiple users attempt to download the same file, they are placed in a queue. Users with higher participation levels are given priority over those with lower participation levels. Thus, a user who shares his files with others will be able to more quickly and easily download the files that he wants from other Kazaa users.

In February 2005, agents in the Cyber Crimes Unit of the Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), obtained a warrant to search Carani's residence. During the search, Senior Special Agent Jason Varda found Carani's computer. It was powered on, connected to the Internet, and running Kazaa at the time. Through Kazaa, Carani's computer was actively downloading files from other Kazaa users, and allowing other Kazaa users to download files on Carani's computer. Agent Varda photographed the screen, which showed that another user was attempting to download a file by the name "incest porn, a little girl has sex with an adult guy." The lower right of the computer screen indicated: "Connected as default user at Kazaa, sharing 214 files."

After photographing the computer screen, Agent Varda disconnected the computer from its power supply. He removed the hard drive and connected it to a write-blocking device to ensure that no data entered the hard drive. Agent Varda then used a software program called EnCase to preview all of the files on the hard drive, including those that had been deleted. The preview revealed a number of suspected child pornography videos.

Agents interviewed Natza during the search. Natza indicated that she and Carani had watched videos of child pornography—sometimes in their entirety on their computer and then deleted them. Meanwhile, Carani agreed to accompany agents to the Highland Park police department. At the station, he was advised of his constitutional rights orally and in writing, and he agreed to be interviewed. Initially, Carani told the agents that he had come across child pornography while searching for adult pornography and had seen it about ten times. He said that when this happened, he would watch the video and then delete it, and that he had never saved any child pornography on his computer. Later, Carani said

that he had seen "tons" of child pornography, and that he may have had one video saved.

The agents took a break from the interview to consult with the United States Attorney's Office. When they returned, Carani admitted that he had not been entirely forthcoming with them. Carani said that he used terms such as "pedo" and "r@ygold" to search Kazaa specifically for child pornography. Agents testified at trial that both of these terms are related to child pornography. Carani also told the agents that the saved video that he had mentioned before the break was titled "Segundo." Carani further indicated that he was particularly interested in videos involving family incest. He stated that he was no longer aroused by adult pornography, and had last viewed child pornography between two weeks and one month prior to the interview. He told the agents that he had never intentionally distributed child pornography, but that he may have done so inadvertently through the Kazaa program as he did not understand what the "My Shared Folder" did.

Carani then prepared the following written statement:

> I have viewed child pornography in the past and then deleted it. I have only one saved right now in the saved section, which is "My Kazaa Lite." As far as computers are concerned I am a beginner at best. I did not distribute any of these videos on purpose, and I have no explanation as to how these videos were shared, but I never shared anything. I don[']t even know how to do so. The only explanation is that, as I viewed them and deleted them, they were automatically shared without my knowing of it. Some of these videos I stumbled upon by accident downloading other videos, and through [curiosity] I looked up some child pornography and again deleted it when I saw it. but the more I saw

> the more I felt that it was wrong to do so. My intentions were never to hurt anybody and forgive my ignorance but I did not know that this was against the law via the way it was done (through Kazaa Lite). I feel extremely bad about what happened, but I can say that I learned a lot through this experience.

Carani's hard drive was sent to Agent Skinner, an ICE forensic analyst with the Cyber Crimes Center in Fairfax, Virginia. Agent Skinner made further use of the EnCase software to analyze the contents of Carani's hard drive. Agent Skinner testified that he initially found two child pornography files in Carani's temporary Internet folders, both "BabyJ Sunshine" files, which he determined had been accessed through a web browser. Agent Skinner used EnCase to search for "BabyJ" references. His search turned up a number of such references, including references to the Kazaa My Shared Folder, and the term "pedophilia." Agent Skinner then constructed a search using a variety of terms associated with child pornography: pedophilia, young Lolita, kiddie, preteen, kindersex, pedo, BabyJ, Baby J, pedo video, illegal pedophilia, r@ygold, underage, incest, Lolita, kiddie porn, real kiddie, kinder, and child lover. This search of the hard drive returned a large number of separate and distinct hits, including 3,050 hits for "kiddie," 2,011 hits for "preteen," 3,603 hits for "pedo," 1,799 hits for "r@ygold," and 3,720 hits for "Lolita." Agent Skinner concluded that Carani was actively seeking out child pornography, as a home computer would not otherwise contain so many references to terms associated with child pornography. Agent Skinner also located numerous files in both the My Shared Folder and the .db folder whose names were suggestive of child pornography. Agent Skinner testified that when a user downloads a file from Kazaa, he is able to view the file name, and when he hovers over the file name, he can see a file description and keywords. Additionally, the Kazaa

screen contains a display which notifies the user that another person is downloading a file from his computer, and indicates which file.

Agent Skinner also testified regarding Carani's Kazaa participation level. Carani's participation level was 771, out of a possible 1,000. Agent Skinner determined that Carani's high participation level was the result of a "hack"—an unauthorized technique which caused Carani's computer to download files from itself, and artificially boost his participation level. Use of the hack required action on the part of the computer user, and there was evidence that the hack had been used extensively. Agent Skinner further testified that Carani's computer and Kazaa program functioned properly.

Carani called Scott Ellis, a computer business consultant, to testify as an expert on his behalf. Ellis testified that Carani was not a sophisticated computer user, and did not know how to use his My Shared Folder on Kazaa. He also testified that a virus, worm, remotely located pedophile, or software glitches could have caused the references to child pornography found on the computer. Ellis described Kazaa as "a piece of rogue software" that "can behave in an uncontrolled fashion." R. 131, p. 464.

Natza and Carani both testified at trial. Each denied making statements to agents that they had watched child pornography, and explained that they only saw child pornography when they mistakenly came across it while searching for adult pornography. They explained that they downloaded video files in large blocks, then reviewed it and discarded the child pornography that they came across. They also emphasized that they were computer novices, and did not fully understand the Kazaa program.

In rebuttal, Agent Skinner testified that his analysis showed that child pornography videos were not down-

loaded in large chunks along with adult pornography; rather, they were downloaded along with other child pornography, in groups of five or six. Agent Skinner also refuted Ellis's testimony that the Kazaa program was not running properly on Carani's computer.

When it came time to instruct the jury, the court used the Seventh Circuit's pattern instructions to define knowingly: "When the word 'knowingly' is used in these instructions, it means that the defendant realized what he was doing and was aware of the nature of his conduct, and did not act through ignorance, mistake, or accident." 7th Cir. Pattern Jury Inst. 4.06. The court also included an instruction on deliberate avoidance, also known as an "ostrich instruction": "You may infer knowledge from a combination of suspicion and indifference to the truth." *Id.* This instruction included an example relevant to this case: "If you find that the defendant had a strong suspicion that a file was child pornography, but ignored that suspicion and downloaded the file, you may conclude that he acted knowingly, as I have used that word." The district court also instructed the jury on the meaning of possession: "In the context of this case, possession means intentionally retaining child pornography after downloading it."

After the jury began deliberations, they sent the following question to the district court: "Does downloading, watching, & deleting constitute possession?" The district court replied: "The answer to this question depends upon whether, at the time he downloaded material, the defendant knew or strongly suspected that it was child pornography and downloaded it anyway. If you find beyond a reasonable doubt that he did, then the answer to your question is 'yes.' If you have a reasonable doubt as to whether the defendant knew or strongly suspected that the material was child pornography at the time he downloaded it, then the answer to your question is 'no.'"

The jury found Carani guilty of possession, but returned a verdict of not guilty as to one of the receipt counts, and was unable to reach a unanimous decision as to the other receipt count.

At the sentencing hearing, the district court heard arguments from both sides. Carani's counsel reiterated his arguments that Carani was not a sophisticated computer user, and that he only downloaded child pornography inadvertently. In support of a distribution enhancement, the government argued that Carani received a "thing of value" as required by the Sentencing Guidelines, by increasing his participation level, which improved his accessibility to other users' files, and that Carani's actions constituted "active trading" in contraband materials. *See* U.S.S.G. § 2G2.2(b)(3)(B).

The district court found that "[t]he defendant's position in regard to whether he knew he possessed child pornography is simply counter to the credible evidence produced at trial, and therefore I do find that the defendant knowingly obtained child pornography on his computer . . . . And turning now to the first guideline issue to which that finding pertains, I do find that the defendant knowingly distributed child pornography in that he knowingly made his child pornography on his computer available to other Kazaa users, who downloaded it from his computer." Mar. 16, 2006 Tr. 38-39. The district court imposed a two-level sentencing enhancement for distribution under U.S.S.G. § 2G2.2(b)(3)(F). The district court added: "A subsidiary finding implied in what I have just said is that the defendant was perfectly aware of the shared files folder. He knew what was in it, he accessed it, and his denial that he knew what was in there is simply not credible." Mar. 16, 2006 Tr. 39. The district court sentenced Carani to 72 months' imprisonment and two years of supervised release.

II. ANALYSIS

This appeal presents three issues: (1) whether the district court abused its discretion by giving the deliberate avoidance "ostrich" instruction to the jury; (2) whether the district court's response to a jury question was in error; and (3) whether the district court improperly applied a sentencing enhancement for the distribution of child pornography.

A. Ostrich Instruction

We review the district court's decision to give an ostrich instruction for an abuse of discretion, viewing all evidence in the light most favorable to the government. *United States v. Leahy*, 464 F.3d 773, 796 (7th Cir. 2006); *United States v. Carrillo*, 435 F.3d 767, 780 (7th Cir. 2006) (citing *United States v. Fallon*, 348 F.3d 248, 253 (7th Cir. 2003)).

An ostrich instruction is appropriate where (1) the defendant claims a lack of guilty knowledge, and (2) the government has presented evidence sufficient for a jury to conclude that the defendant deliberately avoided learning the truth. *Carrillo*, 435 F.3d at 780. Deliberate avoidance is more than mere negligence, the defendant must have "deliberately avoided acquiring knowledge of the crime being committed by cutting off his curiosity through an effort of the will." *Leahy*, 464 F.3d at 796 (citing *Fallon*, 348 F.3d at 253). Deliberate avoidance is not a standard less than knowledge; it is simply another way that knowledge may be proven. *Carrillo*, 435 F.3d at 780 (citing *United States v. Ramsey*, 785 F.2d 184, 189 (7th Cir. 1986)). "The purpose of the ostrich instruction 'is to inform the jury that a person may not escape criminal liability by pleading ignorance if he knows or strongly suspects he is involved in criminal dealings but deliberately avoids learning more exact information about the

nature or extent of those dealings.'" *Carrillo*, 435 F.3d at 780 (quoting *United States v. Craig*, 178 F.3d 891, 896 (7th Cir. 1999); *United States v. Rodriguez*, 929 F.2d 1224, 1227 (7th Cir. 1991)).

Physical acts and outward expressions by the defendant evidencing his deliberate avoidance, while useful, are not necessary for a jury to infer that the defendant was curious but deliberately ignored his suspicions. *Carrillo* 435 F.3d at 780-81 (explaining the difference between avoidance through "overt physical acts" and "purely psychological" avoidance). The circumstances surrounding the defendant may be sufficient to infer that, given what the defendant knew, he must have forced his suspicions aside and deliberately avoided confirming for himself that he was engaged in criminal activity. *Id.* at 781 (citing *United States v. Carrillo*, 269 F.3d 761, 769-70 (7th Cir. 2001); *United States v. Farouil*, 124 F.3d 838, 844 (7th Cir. 1997); *United States v. Stone*, 987 F.2d 469, 472 (7th Cir. 1993); *Rodriguez*, 929 F.2d at 1227-28; *United States v. Caliendo*, 910 F.2d 429, 434 (7th Cir. 1990); *United States v. Josefik*, 753 F.2d 585, 589 (7th Cir. 1985); *United States v. Burns*, 683 F.2d 1056, 1060 (7th Cir. 1982)).

The crux of Carani's argument at trial was that any child pornography videos he may have downloaded to his computer were downloaded solely through inadvertence. In addition to direct evidence that Carani in fact intended to download child pornography, such as statements he made to agents at the Highland Park Police Station, the government also presented evidence from which a jury could infer that Carani deliberately avoided confirming that certain files were in fact child pornography. Government witnesses testified that many files that were, or had once been, on Carani's computer had words associated with child pornography in the file names. Those file names, in addition to file descriptions and keyword

listings, would have been displayed in the Kazaa search listings when Carani downloaded them. These words indicating that the files contained child pornography were, quite literally, right in front of his face. Thousands upon thousands of references to child pornography were found on Carani's computer; and evidence, such as the hack used to boost his participation level, suggests that Carani was not so bungling a computer user as he suggested.

The government presented evidence sufficient for the jury to infer that Carani suspected that files he was downloading and sharing with others contained child pornography, but deliberately pushed those suspicions aside in order to avoid confirming his criminal activities. The district court did not abuse its discretion by giving the ostrich instruction to the jury.

B. Response to Jury Question

"We review a decision to answer a question from the jury as well as the language used in the response for an abuse of discretion." *United States v. Hewlett*, 453 F.3d 876, 880 (7th Cir. 2006) (citing *United States v. Young*, 316 F.3d 649 (7th Cir. 2002)). "[T]he district court retains broad discretion in deciding how to respond to a question propounded from the jury and . . . the court has an obligation to dispel any confusion quickly and with concrete accuracy." *United States v. Sims*, 329 F.3d 937, 943 (7th Cir. 2003). When reviewing the language of a supplemental jury instruction, we consider three factors: "(1) whether the instructions as a whole fairly and adequately treat the issues; (2) whether the supplemental instruction is a correct statement of the law; and (3) whether the district court answered the jury's questions specifically." *United States v. Danford*, 435 F.3d 682, 688 (7th Cir. 2006) (citing *Sims*, 329 F.3d at 943; *Young*, 316 F.3d at 662). An error in a supplemental instruction is only reversible if the

defendant has been prejudiced. *See Young*, 316 F.3d at 662.

Carani argues that, in answering the jury's question about possession, the district court impermissibly lowered the burden of proof with respect to knowledge by including the language, "knew or strongly suspected." Given the jury's confusion on such a critical aspect of the instructions, the district court was within its discretion to provide the jury with an answer. *See Sims*, 329 F.3d at 943.

Having concluded that the district court did not abuse its discretion by providing a supplemental instruction, we must next evaluate the language used in that instruction under the three factor rubric. *See Danford*, 435 F.3d at 688. The first and third factors are easily satisfied. The district court provided a thorough explanation that was specifically targeted at the jury's question regarding whether the defendant "possessed" child pornography if he discarded it after he watched it. The second factor, whether the instruction accurately stated the law, deserves more discussion.

The district court's supplemental instruction indicated that Carani could only be guilty of possession if, "at the time he downloaded material, the defendant knew or strongly suspected that it was child pornography and downloaded it anyway." This definition of possession is surely too narrow.

Suppose that, unbeknownst to an individual, a stranger on the street mistakenly slips a bag of marijuana into his pocket. Moments later, he is arrested on an outstanding warrant and the officer discovers the marijuana. He is not guilty of the possession of marijuana, because he does not have the requisite knowledge. But, suppose that before he is arrested on the outstanding warrant, he discovers the marijuana and decides to keep it. Then,

despite the fact that he did not know about the marijuana at the time that it was put in his pocket, he would have all of the knowledge required to be guilty of possession. *United States v. Myers*, 355 F.3d 1040, 1042 (7th Cir. 2004); *see United States v. X-Citement Video, Inc.*, 513 U.S. 64, 76-78 (1994); *United States v. Hall*, 142 F.3d 988, 997 (7th Cir. 1998) (explaining that if a defendant had the opportunity to delete child pornography files on his computer but chose not to, the requirements of possession have been met).

It is this second scenario that the district court's instructions did not take into account. A possessor of child pornography videos need not know that it is such at the time of download, so long as he discovers that it is child pornography after the download and decides to keep it anyway. The district court's instruction on possession crafted too narrow a definition of possession by requiring knowledge at the time of download.

Thus, the instruction could not have harmed Carani. If anything, Carani benefitted from giving it. In effect, the jury was told not to find Carani guilty of possession if he inadvertently acquired child pornography and subsequently made a conscious decision to keep it. The error in the supplemental instruction was harmless to Carani. Additionally, the use of the term "strongly suspected" in the supplemental instruction was proper given our analysis of the ostrich instruction.

C. Distribution Enhancement

"We review the district court's interpretation and application of the Sentencing Guidelines *de novo*, and its findings of fact for clear error." *United States v. Fife*, 471 F.3d 750, 752 (7th Cir. 2006) (citing *United States v. Ellis*, 440 F.3d 434, 436 (7th Cir. 2006)). "A finding of fact is

clearly erroneous only if, based upon the entire record, we are left with the definite and firm conviction that a mistake has been committed." *United States v. Chamness*, 435 F.3d 724, 726 (7th Cir. 2006) (citations and quotations omitted).

Under U.S.S.G. § 2G2.2(a)(1), the base offense level for possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5) is eighteen. The government requested a five-level enhancement under U.S.S.G. § 2G2.2(b)(3)(B) for the "[d]istribution [of child pornography] for the receipt, or expectation of receipt, of a thing of value, but not for pecuniary gain." The district court, instead, applied a two-level enhancement under U.S.S.G. § 2G2.2(b)(3)(F) for "[d]istribution other than distribution described in subdivisions (A) through (E)." The district court applied a number of other enhancements that Carani does not take issue with, bringing his total offense level to thirty-five. This yields an advisory guidelines range of 168-210 months. The statutory maximum, however, is ten years (120 months). 18 U.S.C. § 2252A(b)(2). Thus, the guidelines provide for a sentence of 120 months. After considering the sentencing factors in 18 U.S.C. § 3553(a), the district court sentenced Carani to seventy-two months' imprisonment followed by two years' supervised release.

Carani makes two arguments with respect to the distribution enhancement: (1) that there was insufficient evidence that he distributed child pornography; and (2) that if he distributed child pornography, he did not do so for the receipt of a thing of value.

This court has not previously considered the exact contours of what constitutes "distribution" in the context of the Kazaa peer-to-peer file sharing program. The Tenth Circuit, however, recently held that allowing others to access one's files through Kazaa is distribution. *United States v. Shaffer*, 472 F.3d 1219 (10th Cir. 2007). The

appellant in *Shaffer*, who was convicted of distributing child pornography, argued that knowing that others were accessing and downloading the files on his computer through Kazaa did not amount to distribution. *Id.* at 1223. Rather, he argued, an affirmative act must be taken by the distributor for each file at the time of distribution. *Id.* The Tenth Circuit rejected this argument, likening distribution through Kazaa to the operation of a self-serve gas station: "The owner may not be present at the station, and there may be no attendant present at all. And neither the owner nor his or her agents may ever pump gas. But the owner has a roadside sign letting all passerby know that, if they choose, they can stop and fill their cars for themselves, paying at the pump by credit card." *Id.* at 1223-24.

The notion that Carani could knowingly make his child pornography available for others to access and download without this qualifying as "distribution" does not square with the plain meaning of the word. Indeed, this court rejected a similar argument in *United States v. Gunderson*, where the defendant had programmed his computer to allow others to access his files if they first uploaded files to his computer. 345 F.3d 471, 473 (7th Cir. 2003). Once the program was written, it required no action by Gunderson to allow others to download his files. *Id.* We described the passive nature of the program as "irrelevant" to whether a distribution enhancement was appropriate. *Id.* Such is the case here. The district court specifically found that Carani made his child pornography videos available through Kazaa, and that he knew other users were downloading these files from him. This finding was not clearly erroneous.

Carani's second argument, that the distribution enhancement was not appropriate because he did not receive a thing of value in return, misstates the record and is a non-starter. At sentencing, the government argued for a five-

level enhancement under U.S.S.G. § 2G2.2(b)(3)(B), which would require that Carani received something of value in return for the child pornography that he distributed. In his opening brief, Carani states: "The court erred by applying the five-level sentencing enhancement under U.S.S.G. § 2G2.2(b)(3)(B)." The record clearly shows that the district court made no such enhancement. The district court applied a two-point enhancement under U.S.S.G. § 2G2.2(b)(3)(F), which does not require that Carani received anything in return for the child pornography he distributed. Thus, there is no factual basis for this argument.

III. CONCLUSION

For the foregoing reasons, Fabio Carani's conviction and sentence are AFFIRMED.

A true Copy:

Teste:

Clerk of the United States Court of Appeals for the Seventh Circuit

EXHIBIT 2

United States Court of Appeals

For the Seventh Circuit
Chicago, Illinois 60604

August 23, 2007

Before

Hon. MICHAEL S. KANNE, *Circuit Judge*

UNITED STATES OF AMERICA, Plaintiff-Appellee, No. 06-2007 v. FABIO CARANI, Defendant-Appellant.	] Appeal from the United] States District Court for] the Northern District of] Illinois, Eastern Division.]] No. 05 CR 150]] John F. Grady,] Judge.

Upon consideration of the **MOTION TO RECALL THE MANDATE**, filed on August 21, 2007, by the pro se appellant,

IT IS ORDERED that the motion is **GRANTED**. The mandate in this case is **RECALLED** and the appeal is **REINSTATED**. The clerk of this court shall file the tendered petition for rehearing and motion to dismiss counsel **INSTANTER**.

EXHIBIT 3

United States Court of Appeals

For the Seventh Circuit
Chicago, Illinois 60604

September 5, 2007

Before

Hon. FRANK H. EASTERBROOK, *Chief Judge*

Hon. MICHAEL S. KANNE, *Circuit Judge*

Hon. ANN CLAIRE WILLIAMS, *Circuit Judge*

No. 06-2007

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

FABIO CARANI,
Defendant-Appellant.

Appeal from the United States District Court for the Northern District of Illinois, Eastern Division.

No. 05 CR 150

John F. Grady,
Judge.

ORDER

On consideration of the petition for rehearing and petition for rehearing en banc, no judge in active service has requested a vote on the petition for rehearing en banc and the judges of the panel have voted to deny rehearing. It is, therefore, ORDERED that rehearing and rehearing en banc are DENIED.

EXHIBIT 4

2/11/05 Fabio Carani 7/25/62
533 Onwentsia
Highland Park I 60035

I have viewed child Pornography in the past and then deleated it. I have only one saved right now in the saved section which is "My Kazaa lite". As far as computers are concerned I am a beginner at best. I did not distribute any of these videos on purpose, and I have no explanation as to how these videos were shared but I never shared anything. I dont even Know how to do so. The only explanation is that, as I viewed them and deleted them, they were automatically shared without my Knowing of it. Some of these videos I stumbled upon by accident, downloading other videos, and through curiousity I looked up some child pornography and again deleted it when I saw it, but the more I saw the more I felt that it was wrong to do so. My intentions were never to hurt anybody and forgive my ignorance but I did not Know that this was against the law via the way it was done (through Kazaa lite). I feel extremely bad about what happened, but I can say I learned alot through this experience

Subscribe and sworn on this date 2/11/05 F.C.

Fabio Carani

GOVERNMENT EXHIBIT 2

[signature] #39595
2/11/05

[signature] #3160
2/11/05

E X H I B I T 5

AFFIDAVIT OF FABIO CARANI

I, Fabio Carani, hereby certify under the penalty of perjury that the following statements are true and correct to the best of my ability, understanding, and belief:

1. That I am the Petitioner so named in my 28 U.S.C. § 2255 motion and its memorandum of law.

2. That the exhibits submitted in support of my § 2255 memorandum are as represented.

3. That at no time did my attorney ever explain to me the risks of proceeding to trial versus pleading guilty. Counsel did tell me that the government had offered a plea agreement. However, counsel never discussed it, or the specifics of the agreement and, in fact, never showed the proposed agreement to me. Rather, counsel just told me not to take it because I would be acquitted at trial. Further, counsel never told me that my handwritten statement amounted to an admission of guilt. And, counsel never informed me that I could receive a higher sentence if I testified at trial and was found guilty. Had counsel sat down and discussed the true risks of proceeding to trial, I would have either accepted the government's plea agreement or entered a plea of guilty without the agreement.

4. To my knowledge, counsel never investigated or researched the Kazaa programs I had on my computer, except to retain an alleged expert on the subject. Counsel never discussed either the program or the expert witness's qualifications with me.

5. None of my counsels ever explained to me the essential elements of any of the counts I was charged with. Thus, I could not

know if the indictment was constructively amended.

6. At no time did any of my counsels ever discuss the concept of a general verdict with me, or what constituted a harmless error versus a structural error. Had these legal terms been explained to me, I would have insisted on raising such a general verdict and/or Sandstrom claim on appeal.

7. At no time was I ever informed by my counsels that the choice of whether or not to testify belonged solely to me. In addition, I was never told that I would be subjecting myself to a harsher sentence if I testified and was found guilty. Instead, counsel simply told me that I had to testify so the jury could hear my defense. Had I known that this decision was mine, and had I been told that I could receive a larger sentence if I testified, I would have never testified.

FURTHER, AFFIANT SAYETH NAUGHT.

Respectfully Submitted on this, the 1 day of DEC, 2007.

Fabio Carani

Fabio Carani
Reg. No. 21827-424
FCI Ashland
P.O. Box 6001
Ashland, Kentucky 41105

EXHIBIT 6

Filesharing Programs and "Technological Features to Induce Users to Share"

A Report to the United States Patent and Trademark Office from the Office of International Relations

Prepared by

Thomas D. Sydnor II

John Knight

Lee A. Hollaar

v 1.1
November, 2006

Foreword

by Jon W. Dudas,
Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office (USPTO)

This report originated when one of its authors showed me data on the behavior of filesharing programs that was being compiled for use in a law review article. Because the data seemed to have potentially important implications, I asked the authors to present it in the form of a report to USPTO. Having reviewed the resulting report, I conclude that this data should be made known to the public.

This report analyzes five popular filesharing programs to determine whether they have contained, or do contain, "features" that can cause users of these programs to share files inadvertently. It concludes that these programs have deployed at least five such "features," and that distributors of these programs continued to deploy such features after their propensity to cause users to share files inadvertently was, or should have been, known. It concludes that further investigation would be warranted to determine whether any distributors who deployed these features intended for them to trick users into sharing files unintentionally.

I requested this report because I believe that it raises important questions about why individual users of these filesharing programs continue to infringe copyrights. This report also reveals that these filesharing programs threaten more than just the copyrights that have made the United States the world's leading creator and exporter of expression and innovation: They also pose a real and documented threat to the security of personal, corporate, and governmental data.

For the Federal Government, this threat became manifest during 2005, when the Department of Homeland Security warned all Federal Agencies that government employees or contractors who had installed filesharing programs on their home or work computers had repeatedly compromised national and military security by "sharing" files containing sensitive or classified data. These users probably did intend to use these programs to download popular music, movies, software or games. But it seems highly unlikely that any of them intended to compromise national or military security for the sake of "free music."

A decade ago, the idea that copyright infringement could become a threat to national security would have seemed implausible. Now, it is a sad reality. It is important to ask how and why this happened. This report attempts to provide some answers and to encourage further research into questions that it can raise, but not answer.

The unanswered questions raised by this report implicate diverse competencies: Some might be best addressed by consumer-protection advocates or agencies, others by computer-science researchers. By releasing this report, I hope that USPTO will

encourage others to bring their expertise to bear on some of the questions that this report leaves open. Examples of such questions might include the following:

- What is the overall prevalence of inadvertent sharing? It may be possible to estimate the number of users who have recursively shared "C:\" or their "My Documents" folder, but estimating the number of users inadvertently sharing downloaded files or their "My Music" folder might be much more difficult.

- How can users of filesharing programs who do not want to upload files *effectively* avoid the sort of coerced-sharing features discussed in this report?

- What are the best options for owners of home computers who want to avoid the security and liability risks associated with filesharing programs?

Finally, I reviewed this report as both a father who manages a home computer and the director of a Federal Agency that must protect the security of valuable electronic files and data. It leads me to believe that I owe a debt of thanks not only to my colleagues at the Department of Homeland Security, but also to two groups of persons.

First, I would like to thank all of the computer-science researchers who have studied filesharing networks. They have done what scientists are supposed to do: Observed carefully and reported what they found—both the good and the bad. Their reports bring to the debate about filesharing objectivity and dispassion that has otherwise been lacking.

I would also like to thank the researchers, reporters, agencies, private citizens, and information-security firms who worked for years to call attention to the persistent and recurring problem of inadvertent sharing. Special thanks are owned the unnamed Samaritan interviewed by CBS News, to the creator of the website *See What You Share*, and to Dr. Howard Schmidt and the employees of Tiversa, Inc.

Table of Contents

I. Executive Summary.

For years, computer-science researchers, Federal Agencies, concerned private citizens, IT-security companies, public-interest groups, news reporters, and others have also reported that users of popular filesharing programs have been sharing files unintentionally. More recently, in *MGM Studios, Inc. v. Grokster, Ltd.*, the Supreme Court found "unmistakable" and "unequivocal" evidence that distributors of two popular filesharing programs intended to induce users of their programs to infringe copyrights. The findings in *Grokster* suggest that persistent reports of inadvertent sharing could signal the effects of duping schemes, a known means of inducement.

In a duping scheme, an entity that intends to use others as a means to achieve an illegal end tricks other people into inadvertently or unintentionally performing a potentially illegal act. In the context of filesharing, duping schemes could be particularly effective. Duping that caused infringing files to be shared inadvertently by young, new or unsophisticated users could still make millions of files available for downloading. Indeed, new users of filesharing programs tend to download many more files than established users, so duping that targeted new users could add a disproportionately large number of files to the network. Duping schemes that targeted young or unsophisticated users would also ensure that attempts to enforce copyrights against those infringers who upload hundreds or thousands of infringing files would tend to target young or sympathetic users.

This report reviews public data about the behavior of five popular filesharing programs; it focuses on the programs BearShare, eDonkey, KaZaA, LimeWire, and Morpheus. It seeks to answer two questions. *First*, have distributors of these filesharing programs deployed features that had a known or obvious propensity to trick users into uploading infringing files inadvertently? *Second*, if so, do the circumstances surrounding the deployment of such features suggest the need for further investigation to determine whether any particular distributor *intended* for such features to act as duping schemes—as "technological features to induce users to share."

This report concludes that the distributors of these five filesharing programs have repeatedly deployed features that had a known propensity to trick users into uploading infringing files inadvertently. Distributors deployed at least five such features:

- **Redistribution features**: All five programs analyzed have deployed a feature that will, by default, cause users of the program to upload (or "share") all files that they download. These features create a counter-intuitive link between downloading files for personal use and distributing files to strangers, and they have often been implemented in ways that could make their effects less obvious to new users. Since 2003, lawsuits against users of filesharing programs have made it more important for users to understand the effects of redistribution features. During this period, some programs tended to disclose less information about their redistribution features.

- **Share-folder and Search-Wizard Features**: All five programs analyzed have deployed share-folder or search-wizard features. These features are uniquely dangerous: They can cause users to share inadvertently not only infringing files, but also sensitive personal files like tax returns, financial records, and documents containing private or even classified data. Published research identified these features as causes of inadvertent sharing by mid-2002. By mid-2003, the distributors of the programs analyzed here had agreed to discontinue use of these features, and concerned legislators had warned that their continued use would compromise national security because government employees using these programs would inadvertently share files containing sensitive or classified data.

  Nevertheless, the distributors of BearShare, eDonkey, LimeWire and Morpheus programs kept deploying search-wizard or share-folder features, and the distributors of KaZaA eliminated these features in a way that would tend to perpetuate inadvertent sharing previously caused by such features. By late spring of 2005, the Department of Homeland Security reported that government employees using filesharing programs had repeatedly compromised national and military security by "sharing" files containing sensitive or classified data.

  - **Share-folder features**: All five of the programs analyzed have deployed a feature that lets users store downloaded files in a folder other than the specially created folder that stores downloaded files by default—but does so through an interface that does not warn users that all files stored in the selected folder will be shared. In most cases, the sharing caused by this feature will be recursive: The program will share not only the files stored in the folder selected to store downloaded files, but also all files stored in any of its subfolders.

  - **Search-wizard features**: At least three of the programs analyzed have deployed a feature that will search users' hard drives and "recommend" that users share folders that contain certain "triggering" file types, which usually include document files, audio files, audiovisual files, and image files. Some search-wizard features activate automatically; others require the user to trigger them. Some are activated during a program's installation-and-setup process; others are an option that a user can activate after the program is installed and running. Some will select identified folders for sharing; others "recommend," but do not select, identified folders for sharing. All search-wizard features discussed will cause recursive sharing of identified or selected folders.

- **Partial-uninstall features**: At least four of the programs analyzed have deployed partial-uninstall features: If users uninstall one of these programs from their computers, the process will leave behind a file that will cause any subsequent installation of any version of the same program to share all folders shared by the "uninstalled" copy of the program. Whenever a computer is used by more than one person, this feature ensures that users cannot know which files and folders these programs will share by default.

- **Coerced-sharing features**: Four of the programs analyzed have deployed features that make it far more difficult for users to disable sharing of the folder used to store downloaded files. This folder may be the default download folder created by the filesharing program or an existing folder selected to store downloaded files through a share-folder feature. In each case, the feature can provide misleading feedback indicating—incorrectly—that the user has disabled sharing of the download folder. But in each case, an obscure mechanism appears to allow sophisticated users to avoid the coerced-sharing feature and stop sharing the download folder.

All five of these features can cause users to share infringing files inadvertently. Redistribution and coerced-sharing features can cause users to share *downloaded* files inadvertently: As *Grokster* noted, these files are usually infringing. Share-folder, search-wizard, and partial-uninstall features can cause users to inadvertently share *existing* files on their computers: The design of these features ensures that the files shared may tend to include users' collections of media files, like audio files copied from purchased CDs.

All five programs analyzed in this report have deployed most or all of these features during at least some portion of the period from 2003 to 2006. In many cases, versions of these features actually became more aggressive after their propensity to cause inadvertent sharing was, or should have been, known to reasonable distributors of filesharing programs. For example, the distributors of BearShare, eDonkey, LimeWire and Morpheus began or continued to deploy poorly disclosed redistribution features, share-folder features, search-wizard features and/or coerced-sharing features even after these distributors drafted a *Code of Conduct* that should have precluded use of any such features. Some distributors even responded to reports of inadvertent sharing by releasing new versions of their programs that seemed improved, but actually *perpetuated* inadvertent sharing caused by features previously deployed. Consequently, this report concludes that the totality of the circumstances surrounding the deployment of such features justify further investigation to determine whether particular distributors *intended* for such features to act as duping schemes.

This report does not, however, draw conclusions about the intent of any particular distributor that deployed some or all of these features in its filesharing program. This report analyzes public data, and it is possible that nonpublic data now controlled by a particular distributor might show that it deployed these features mistakenly, negligently, or recklessly. This limitation on the scope of this report's conclusions is a precautionary measure: It does not imply that a court obligated to draw conclusions about the intent of a particular distributor could not find that the data discussed herein provides "unmistakable" or "unequivocal" evidence of intent to induce copyright infringement within the meaning of *MGM Studios, Inc. v. Grokster*, 125 S. Ct. 2764 (2005).

II. Background.

A combination of two factors suggested the need for the analysis conducted in this report. *First*, on June 27, 2005, in *MGM Studios, Inc. v. Grokster, Ltd.*, the Supreme Court of the United States found "unequivocal" and "unmistakable" evidence that the distributors of the Grokster and Morpheus filesharing programs intended to induce users of their programs to infringe copyrights. Duping schemes are a known means to induce others to perform illegal acts.

Second, in the context of filesharing, duping schemes would, by definition, cause users of filesharing programs to share infringing files unintentionally. For years, researchers, governments, the media, and users themselves have been reporting that users of some filesharing programs end up "sharing" files unintentionally.

Together, these two factors suggest a need to investigate to determine whether distributors of filesharing programs may have used duping schemes to induce users of their programs to upload, or "share" infringing files unintentionally.

A. Policy and practical considerations show the need to consider whether distributors may have designed filesharing programs to dupe new or vulnerable users into "sharing" infringing files.

The inducement doctrine reaffirmed by the *Grokster* Court has long been a basis for imposing secondary civil liability for many forms of wrongful conduct, including copyright, patent, and trademark infringement. As a result, inducement cases and laws provide courts, rightsholders and technologists with "diagnostic tools" that can identify conduct that may indicate intent to induce others to break the law.

For example, in cases involving alleged infringements of intellectual-property rights, courts have called inducement the civil analog of the criminal-law doctrine of aiding and abetting. By analogy, the two-part structure of the criminal aiding-and-abetting statute, (Section 2 of the United States Criminal Code), suggests that there are two means for a culpable entity to induce others to commit illegal acts:

- **Section 2(a) Inducement (Persuasion):** An entity might seek to persuade or encourage third parties to break the law *intentionally*. In the context of filesharing, a distributor engaged in 2(a)-type inducement might say something like this: "Separating the download of the data and the keys may help protect file sharers from lawsuits, making it more difficult for courts to say exactly which party is responsible for copyright infringement...."[1]

- **Section 2(b) Inducement (Duping Schemes):** An entity might also seek to dupe or trick third parties into breaking the law *unintentionally or unwittingly*. Justice Story's classic example of duping involves a murderer who has food poisoned and delivered by a child who does not intend to harm the intended victim.[2] In the context of filesharing, "duping schemes" might be executed by features in

filesharing programs that trick some users into sharing files that they did not intend to make available to others.

The difference between inducement-by-persuasion and duping turns on whether the person induced to perform a potentially illegal act *intended* to break the law—not on the use of deceit. For example, inducement-by-persuasion might well involve deceit: An inducer might misrepresent the odds of getting caught in order to persuade another person to perform an illegal act intentionally. The *Grokster* decision focused on evidence suggesting that distributors of filesharing programs encouraged users of their programs to infringe copyrights intentionally. The Court did not consider the possibility of duping.

After *Grokster*, it becomes important to consider the possibility of duping. In any context, duping schemes can be particularly destructive to the rule of law:

- Duping schemes can conceal their authors: Violations of the law occur, but they seem to result from the mistakes or negligence of third parties.
- Duping schemes can also endanger unwitting participants: Persons duped may risk civil liability or even criminal prosecution.
- Duping schemes can also shield the culpable: A duping scheme also encourages culpable parties to break the law intentionally; if culpable lawbreakers are caught, they can avoid or minimize the consequences of their acts by posing as dupes.

While duping schemes might seem appealing, they have remained rare in practice. Ordinarily, it would be unlikely that distributors of a product would have incentives to dupe its users into breaking the law. And even if distributors had such incentives, two factors would usually deter a resort to duping.

First, consumers usually have very powerful remedies against the distributors of any product that causes any sort of foreseeable harm. The vast information markets that surround almost all popular consumer products would also be likely to detect and reveal any wrongdoing—and thus ensure that the remedies available to consumers would be brought to bear.

Second, duping schemes could reveal themselves if they affect too many users of a product: If most people who use a product end up breaking the law unintentionally, it will become obvious that the product—and its designers—have contributed to this result. Duping would thus have to be calibrated to cause only a relatively small subset of users to break the law. Consequently, duping should occur only if some disproportionate benefit could be gained by tricking only a relatively small percentage of users into breaking the law.

Filesharing presents an unusual context in which these practical obstacles to duping diminish. In practice, popular filesharing programs are used mostly to download and upload infringing copies of copyrighted music, movies, games, images, and software. For example, in *Grokster*, unrebutted evidence indicated that 90% of the files available

on filesharing networks consisted of infringing files. Upon remand, the district court in *Grokster* found that undisputed evidence showed that "[a]lmost 97% of the files actually requested for downloading were infringing or highly likely to be infringing."[3]

When almost all users of a product use it to break the law almost all of the time, the protections against duping provided by consumer-protection and tort laws recede. As a practical matter, persons who use a filesharing program to download infringing files cannot call their state attorney general or the Federal Trade Commission and report the following complaint: "I installed this program so I could download popular music without paying for it, but the program caused me to share the infringing files that I downloaded, and that got me sued." The user who did this might well be confessing to a federal crime. Nor would this user be a sympathetic tort plaintiff.

This situation also seems to deter information markets: For example, because virtually everyone who uses a popular filesharing program appears to use it almost exclusively to download infringing files, a mazagine or website seeking to do a meaningful review of filesharing programs would have to assess their relative efficacy as a means of copyright piracy. Perhaps for this reason, filesharing programs have become one of the most widely used, let least discussed and reviewed, computer programs on the market.

Filesharing also presents the unusual case in disproportionate benefits could be gained by tricking only new, unsophisticated or young users of filesharing programs into sharing infringing files:

- Filesharing programs are very widely used. Duping could thus cause many millions of files to be uploaded even if it affected only a small fraction of users.

- New users of filesharing programs download many more files than existing users.[4] Duping that affected only new and unsophisticated users would thus be disproportionately effective at adding files to a network.

- Many users of filesharing programs are young teenagers or preteen children.[5] Children are the classic targets of duping.

Taken together, these three factors suggest that schemes to dupe young, new, or unsophisticated users of filesharing programs into sharing infringing files unintentionally could help populate networks with infringing files even if they affected only a small percentage of users.

An additional factor could then allow duping schemes to have a uniquely malign effect: Were a distributor to design its filesharing program to dupe otherwise-sympathetic users into "sharing" many infringing files unintentionally, the distributor responsible would not be the one to punish these users for their credulity. As a result, duping schemes might tend to vilify—not their authors—but copyright holders and copyright laws. Copyright holders trying to deter infringement might sue the most egregious infringing users of filesharing programs—those few who upload hundreds or thousands of infringing files.

Duping schemes could ensure that such lawsuits would actually tend to target a program's youngest and most sympathetic users.

Such a situation would raise important policy concerns. Historically, copyrights have generally been enforced against *distributors* or *commercial users* of protected works, but not against ordinary consumers. This long practice ensured that copyrighted works could be enjoyed by everyone—from toddlers to seniors—without the need for any detailed knowledge of copyright law.[6]

Filesharing became the exception to this practice because many programs were designed to ensure that infringing use of filesharing networks could not be halted by sending takedown notices to the distributors of the programs that create them, or even by suing those distributors into bankruptcy. After the *Napster* litigation, distributors were told that such designs could help *them* avoid liability: "The key here is to let go of any control you may have over your users—no remote kill switch, contractual termination rights or similar mechanisms."[7] Thus, even if rightsholders successfully sue the distributors of these programs, they still confront a lose-lose-lose decision: They must either (1) try to deter infringement by suing the consumers who use these programs, (2) try to deter infringement by paying off the architects of filesharing piracy, or (3) accept ongoing, pervasive infringement that could eventually waive their rights to prevent unauthorized reproduction or distribution of their works.

In *Grokster*, the Supreme Court noted, "[T]he ease of copying songs or movies using software like Grokster's and Napster's is fostering disdain for copyright protection." Network architecture that forces copyright holders to waive their rights, payoff pirates, or sue consumers may inevitably foster further disdain for copyright protection—for the system of private property rights in expressive works that the Framers of the Constitution thought indispensable to the growth of private expression in a democratic republic.

Indeed, after some copyright holders sued users uploading many hundreds or thousands of infringing files, defenders of filesharing objected that such users tend to be poor, unsophisticated, or children. For example, in its 2005 report, *RIAA v. The People*, the Electronic Frontier Foundation (EFF) described the users uploading many hundreds of infringing files as follows: "The[y] were not commercial copyright pirates. They were children, grandparents, [and] single mothers...." EFF then cited numerous individual cases involving users who were (1) unaware that sharing infringing files was illegal, (2) unaware that they were uploading infringing files that they had downloaded, (3) poor, (4) unsophisticated, (5) children or young teenagers, or (6) some or all of the above.[8]

The cases cited by EFF involve defendants who seem sympathetic *because* circumstances strongly suggest that they never intended to turn their home computers into online distribution centers for pirated goods. Another EFF lawyer condemned enforcement against such users as a "reign of terror" against "defenseless people" who probably did not intend to break the law—"any real pirate would never leave the meta-data and would be using someone else's Internet access."[9] But such condemnations just beg a more fundamental question: *Why* do children, grandparents, and poor single mothers end up sharing hundreds or thousands of infringing files inadvertently?

Distributors of filesharing programs have also argued that the prevalence of children among high-volume uploaders of infringing files makes it wrong for copyright holders to enforce their rights. For example, one high-volume uploader of over 800 infringing audio files turned out to be a 12-year-old female honor student receiving public assistance. The distributors of the BearShare, Morpheus, and eDonkey programs responded to this tragic situation in the press release *Peer-to-Peer Trade Group to RIAA Bullies: Come Out and Fight Us If You Want, But Leave the Little Guys Alone*:

> [I]t's time for the RIAA's winged monkeys to fly back to the castle and leave the Munchkins alone....
>
> They're playing the Wicked Witch of the West, using $150,000-per-song lawsuits to frighten the little people....
>
> Like the Cowardly Lion, the record industry bullies should come out and fight us if they want, but leave the little guys alone.[10]

Such rhetoric heightens the need to investigate. Distributors of filesharing programs created an unprecedented, avoidable, and tragic conflict between artists and their fans. These distributors then denounced the enforcement lawsuits against users that their own choices had made nearly inevitable. But declarations of sympathy for the fate of the "little guys" would ring very hollow if authored by distributors deploying "features" that could tend to cause "the Munchkins" to become high-volume uploaders of infringing files.

These policy considerations show why it is important to consider the possibility of duping. They are also reinforced by practical considerations. By definition, duping schemes would cause users of filesharing programs to "share" (or "upload") infringing files *unintentionally*. For years, an expanding set of public reports has asserted that users of filesharing software do "share" files unintentionally.

Since at least 2002, such reports have come from computer-science researchers, congressional hearings, agencies, consumer groups, scholars, security companies, news media, and users of filesharing programs. These reports have arisen from sources on both sides of the filesharing debate and sources largely unconcerned with that debate. While these reports do not—and cannot—describe the full scope of the problem, they show that unintentional sharing of files has recurred regularly. In the aftermath of *Grokster*, the potential implications of such reports become clear enough to warrant investigation.

B. This report investigates whether popular filesharing programs contain features that their distributors knew or should have known could cause users to upload files inadvertently.

Appendix A provides more detail about the factors that shaped the scope of this report, and it defines some of the terms used. Consequently, this section will simply outline the

scope of the issues that this report addresses. This report reviews only publicly available data, and it seeks to answer two questions.

First: Do popular search-and-download filesharing programs contain—or have they contained—features that can cause users to share files unintentionally? This report will focus on five such programs: KaZaA, LimeWire, BearShare, eDonkey, and Morpheus.[11] It will examine how the sharing-related features of these programs operate, and how their operation did or did not change from 2002 through 2006.

Second: Do the circumstances surrounding the use of any such features suggest a need to further investigate whether any particular distributor that deployed such a feature *intended* for it to dupe users into sharing files inadvertently? This report does not purport to determine whether any particular distributor intended to dupe users by deploying a feature with a known or obvious propensity to cause inexperienced users to share files inadvertently. To be sure, intent might be inferred from unrebutted public data showing that a particular distributor deployed a feature that had a known propensity to cause users to share files inadvertently. But even in such a case, a distributor might possess nonpublic data that would tend to show that the feature at issue was actually deployed innocently, negligently, or recklessly.

It is important to note that a report that seeks to answer the two questions described above will not answer many other important questions. Filesharing programs raise an array of public-policy and public-safety concerns, and only a few of them will be addressed in detail in this report.

This report focuses on features that could mislead users into *sharing files* inadvertently: It does not discuss features that might dupe users into performing other actions. For example, by default, most filesharing programs make a user's computer eligible to serve as a "supernode" or "ultrapeer." It seems highly unlikely that most users realize that this means that they have "agreed" to house—on their computers—search-index servers much like those that subjected Napster, Inc. to billion-dollar secondary liability or those that subjected operators of Direct Connect "hubs" to criminal prosecution and conviction.[12] Nevertheless, housing a search-index server does not cause users to share their own files inadvertently, so the issue will not be discussed further here.

This report also focuses on features that could indicate intent to dupe users into sharing files *inadvertently or unintentionally*: It does not discuss features in popular filesharing programs that encourage users to sharing infringing files *intentionally*. Many potential examples of such features exist:

- Versions of the KaZaA filesharing program contained a "Participation Level" feature that creates strong incentives for users to share files that other users want to download. As *Grokster* notes, such files strongly tend to be infringing.

- Professor Strahilevitz argues that filesharing programs encourage new or unsophisticated users to share files through "charismatic code" that "presents each member of a community with a distorted picture of his fellow community

> members by magnifying cooperative behavior and masking uncooperative behavior." Deceit gives this code its "charisma": "While there is nothing terribly persuasive about telling a lie per se, the genius of Gnutella is the way in which it makes that lie look like a reality to its users."[13]

Under *Grokster*, such features might be relevant to an analysis of inducement-by-persuasion. Nevertheless, features that encourage users to *intentionally* share infringing files do not suggest duping, so they are not a focus of this report.

Finally, this report does not assess *all* security risks associated with filesharing programs. At least two types of security risks fall outside of its scope. First, filesharing programs themselves may contain bugs or flaws that hackers can exploit to compromise computers or networks. Second, filesharing programs can download mislabeled files that contain malicious code that can compromise computers and networks. These vulnerabilities are significant, but neither is a focus of this report.

III. An Analysis of Potential "Technological Features To Induce Users to Share" in Five Popular Filesharing Programs.

A potential link between filesharing programs and duping schemes first appears in the 2000 study *Free Riding on Gnutella*, one of the most widely cited scientific studies of post-*Napster* filesharing networks.[14] In 2000, early filesharing programs based upon the Gnutella protocol had similar uploading and downloading capabilities: A user had to make a conscious decision and act affirmatively in order to download or upload any particular file.[15]

Researchers from Xerox PARC Labs studied the resulting network in August of 2000 and concluded that Gnutella-based networks would not be robust, efficient or scalable because so few users chose to share files: 66% shared no files at all, so 1% of all users provided 47% of all responses to queries for files. The Gnutella network, though entirely decentralized in its architecture, thus remained highly centralized in fact.

Free Riding on Gnutella and subsequent research also noted that these low levels of sharing were no accident: Design characteristics like anonymity, indiscriminate sharing, large user-bases, dynamic membership, cheap pseudonyms, and lack of central administration made filesharing networks suitable for infringing use, but these features also discouraged users from sharing files.[16] Indeed, they ensured that few users would possess *any* files that they could safely and legally distribute over filesharing networks.

For example, many parents will *want* to share digital photos of their children with family and friends. But "sharing" such photos over a filesharing network would be ineffective and dangerous. LimeWire has explained why it could be ineffective: "Here's modern p2p's dirty little secret: It's actually horrible at [locating] rare stuff."[17] It would be dangerous because the anonymity, cheap pseudonyms, and indiscriminate sharing that make these networks an attractive venue for infringement also attracted "unstoppable" pedophiles who share violent child pornography, and, reportedly, inadvertently shared

data about particular children.[18] In short, if users of filesharing programs were not sharing files, the distributors of these programs had their own design decisions to blame.

From their analysis, the authors of *Free Riding* drew the following conclusions:

- The Gnutella network faced "possible collapse" if developers of Gnutella-based programs continued to rely on "voluntary cooperation between users."
- Developers of Gnutella-based programs could rely, instead, on "technological features to induce users to share."[19]

The study noted at least two such "features." One was the redistribution feature used by Napster, Inc. that would cause users to upload files downloaded from the network. Another was the forced-sharing feature used by FreeNet that compels each user to store and share files.

The phrase "technological features to induce users to share" is inherently interesting in a post-*Grokster* world. In itself, it might not suggest duping: Distributors could "induce" users to share noninfringing files or to share infringing files intentionally. But this phrase does suggest duping when reliance upon "technological features to induce users to share" is presented as an alternative to reliance upon "voluntary cooperation between users." Consider, for example, the most widely deployed "technological feature" cited by *Free Riding on Gnutella*: A redistribution feature that will, by default, cause users to upload (or "share") all files that they download.

A. Redistribution features can cause users to share infringing downloads unintentionally.

After *Free Riding on Gnutella* was published, the redistribution features it recommended became nearly ubiquitous in filesharing programs. Some distributors reportedly implemented such features in response to its findings.[20] By 2002, the Gnutella protocol required compliant filesharing programs to contain a redistribution feature.

Research suggests dramatic results: By mid-2001, another study of the Gnutella network revealed that only 25% of studied users shared no files.[21] A smaller 2001 study of users of versions of the KaZaA and Morpheus filesharing programs that contained redistribution features showed that only 32% of those users shared no files: "At least part of this increased sharing, relative to Gnutella, surely stemmed from the defaults built into these systems."[22]

Today, almost all popular filesharing programs contain a redistribution feature. Most programs implement this feature by storing downloaded files in a folder that is shared by default. As *Free Riding on Gnutella* predicted, distributors of filesharing programs assert that these redistribution features are essential. In a 2004 letter to six Senators, the distributors of KaZaA asserted that disabling KaZaA's redistribution feature would

"cripple" the KaZaA network. In an internal email, Altnet asserted that "p2p exists because of this feature."[23]

Obscure or poorly disclosed redistribution features that tend to cause new or unsophisticated users to share downloaded files inadvertently could assist filesharing networks in two ways. First, they could help networks scale by ensuring that popular downloads are widely shared. Second, they would ensure that more users would share files with the same hash value: This would facilitate "swarming" downloads in which users download pieces of the same file simultaneously from multiple sources.[24]

Commentators have repeatedly concluded that redistribution features cause users to "share" downloaded files unintentionally. For example, in 2003, Professor Strahilevitz concluded that these features cause "unsophisticated or ambivalent users to make their files available for others to download."[25]

Similarly, in 2004, a neutral *amicus* brief to a Federal court from five professors of intellectual-property law from Harvard Law School's Berkman Center for the Internet and Society concluded that "only the most sophisticated" high-volume uploaders of infringing files intend to share *any* files: "Many users may not be aware that redistribution is automatically enabled by default." These scholars warned that distributors create "technological barriers" to ensure that "disabling file-sharing ... can be [a] very difficult, and perhaps impossible, task for all but the most expert computer users."[26]

Professor Sag drew similar conclusions: "[P]eer-to-peer networks are programmed to create strong incentives to upload.... In part, this is achieved by burying the pro-sharing default so that it takes some user sophistication to figure out how to turn it off."[27]

These conclusions accord with reports from users of filesharing programs. Beginning in mid 2003, some copyright holders began suing users of filesharing programs alleged to be uploading many hundreds of infringing files. Sued users soon reported that they did not know that they were "sharing" the files that they had downloaded. The pro-filesharing website *p2pnet.net* characterizes their complaints as follows:

> It seems most of the RIAA's victims, including young children, used KaZaA.... They also say Sharman failed to make it clear that the folder in which KaZaA downloads were stored needed to be disabled so other people couldn't tap into it. But even if they had known, figuring out how to disable the folder was beyond them, say victims, especially children.[28]

While several of these sources explain why users might have difficulty disabling redistribution features, none explains why users might overlook redistribution features. But *Free Riding on Gnutella* shows that most users of filesharing programs do not want to share files; they only want to download files shared by others. For two reasons, users who only want to download can overlook a program's redistribution feature.

First, users who only intend to download files have no incentive to explore the sharing-related interfaces of their filesharing programs. Filesharing programs typically disclose their redistribution features in these sharing-related interfaces.

Second, redistribution features link the acts of downloading and uploading in a way that can be profoundly counterintuitive to consumers generally or even to experienced computer users. Ordinarily, the act of acquiring a book, CD, or DVD for personal use does not cause a consumer to distribute that work to others. One user who lost her life savings in a lawsuit stressed this point:

> I never willingly shared files with other users.... [T]he music I downloaded was for home, personal use. ... As far as I was concerned copyright infringement was what the people in Chinatown hawking bootlegged and fake CDs on the streetcorner were doing. ...[29]

This user understood that distributing unauthorized copies of protected works constitutes infringement, but she did not understand that the redistribution feature in her filesharing program ensured that she was doing just that.

Redistribution features could even confuse experienced computer users: Most programs do not cause their users to automatically redistribute saved or downloaded files. For example, using an Internet browser to visit websites or download files does not cause the user to begin acting as a server for each visited website or to begin making each downloaded file available to strangers.

By late 2003, distributors of filesharing programs knew or had reason to know that disclosing redistribution features only in sharing-related interfaces could cause users to share downloaded files inadvertently. Many distributors pledged to improve their disclosures. For example, by October of 2003, the distributors of eDonkey, BearShare, LimeWire, and Morpheus had drafted and published a *Code of Conduct* that required their programs to "conspicuously require the user to confirm the folder(s) containing the file material that the user wishes to make available to other users before making such material available..."[30]

This conspicuous-confirmation requirement permits redistribution features—if they "conspicuously require the user to confirm" that he or she wishes to share downloaded files. Although the distributors of BearShare, eDonkey, LimeWire, and Morpheus all pledged to comply with this *Code* and repeatedly represented that they had done so, studied versions of their programs did not "conspicuously" require users to confirm that they wished to share downloaded files.[31] Indeed, disclosure of redistribution features often *decreased* after the *Code* was drafted.

Three basic patterns of disclosure emerge. The first is nondisclosure: A program might provide new or download-only users with no information that would suggest that a redistribution feature exists. For example, studied versions of eDonkey, like version 1.4.3, provide no information about sharing on their main interface—by default or otherwise—nor do they disclose their redistribution feature during their installation-and-

setup processes.[32] eDonkey 1.4.3 did not "conspicuously require the user to confirm" that she wished to share downloaded files by default.

But nondisclosure is better than a potentially misleading disclosure: A program containing a redistribution feature could suggest that redistribution was disabled by default. Here, for example, is an interface that appears during the installation-and-setup process in a 2003 version of Morpheus:

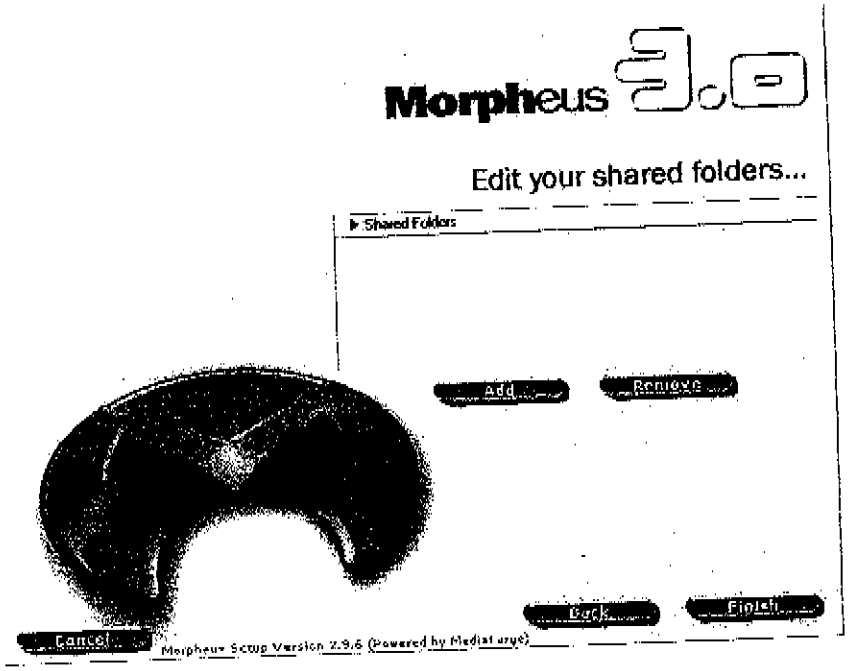

Figure 1: Morpheus 3.0.36

This version of Morpheus appears to lack a redistribution feature. Big black text tells the user, "Edit your shared folders", and the list below is empty by default. But appearances can deceive: This version of Morpheus has a redistribution feature—downloaded files are stored in a specially created "Downloads" folder that will be shared by default. Consequently, the information provided could be affirmatively misleading. Nor has this interface improved materially in the more recent versions of Morpheus.

Finally, other disclosures decreased over time. Information can be disclosed in ways that make it too ambiguous to be useful. For example, in THE HITCHHIKER'S GUIDE TO THE GALAXY, aliens create a supercomputer called Deep Thought to calculate the meaning of life, the universe, and everything. After calculating for ages, Deep Thought discloses that the answer to the meaning of life, the universe and everthing is "42." Just "42." This disclosure does not really illuminate the meaning of life.

Fortunately, real-world filesharing programs have provided main-interface disclosures about sharing more useful than the information provided by the fictional computer Deep Thought. One of the best of these displays appears in 2003 and 2004 versions of LimeWire. This display appeared at the bottom left of the main interface:

Figure 2: LimeWire 4.0.7

This display is not perfect: It does not clearly inform the user that *they* are the one sharing these files. Users migrating from KaZaA might find this ambiguity particularly confusing because the lower left of the KaZaA main interface provides information about files shared by *other* users of the KaZaA program. Nor does this display reveal how the user might disable the sharing disclosed. Nevertheless, this display could provide useful information to some users and with minor modifications, it might have been even more informative.

Given that this best-of-class display could have easily become even more useful and informative, one might wonder whether it has changed over time. It has. In early 2006, this display looked like this:

Figure 3: LimeWire 4.10.9

"42." Just "42." In other words, this user is sharing 42 files. LimeWire's once-useful display became a real-world implementation of Deep Thought.

In summary, some programs disclosed less information about their redistribution features after the filing of copyright-enforcement lawsuits made this information more important to users. This suggests that redistribution feature can cause new or unsophisticated users to share downloaded files inadvertently. But as potential duping schemes, redistribution features would have two weaknesses.

First, redistribution features are not really that difficult to detect or disable. While the deployment of redistribution features may have radically increased users' propensity to share files in 2001, their effects soon faded: For example, a study using data collected in mid-2002 reported that 42% of studied Gnutella users shared no files.[33]

Second, redistribution features cannot add new content to a network. In particular, they cannot cause users to inadvertently share the large collections of *existing* media files stored on their computers, (such as those copied from purchased CDs).[34]

Consequently, a distributor might deploy other "technological features to induce users to share" that would compensate for these inherent weaknesses of redistribution features. It thus becomes important to determine whether popular filesharing programs have contained, or do contain, features that could cause users to inadvertently share *existing* files already stored on their computers.

All five programs examined have contained such features. Many still do.

B. Search-wizard and share-folder features can cause users to infringe copyrights—or jeopardize their own financial or personal safety—by sharing existing files inadvertently.

In mid-2002, computer-science researchers from HP Labs showed that distributors of filesharing programs had deployed two features that could cause users to inadvertently share existing files stored on their computers:

- **Search-wizard features**: Search wizards may activate automatically, or they may be activated by the user. When activated, these features scan portions of a user's hard drive and then identify folders that contain "triggering" file types, which usually include audio files, audiovisual files, and document files. A list of identified folders is then displayed. Some search wizards merely recommend sharing of listed folders—these folders will be shared only if the user checks an associated checkbox. Others will automatically select all listed folders for sharing. Search wizards were often included in filesharing programs' installation-and-setup processes; they may also be accessed from menus within the programs.

- **Share-folder features**: By default, most filesharing programs store downloaded files in a folder created by the program during installation. A share-folder feature lets the user select a different folder to store downloaded files. But it does so through an interface that does not clearly warn the user that the selected folder, and usually its subfolders, will be "shared" with other users.[35]

These search-wizard and share-folder features usually cause *recursive sharing*: They will "share" not only the files stored in a folder selected by a search-wizard or share-folder feature, but also files stored *in any subfolder* of the selected folder. In short, a recursive-sharing search-wizard or share-folder feature treats a user's instruction to store files in, or share, one folder as an authorization to share that folder and many other folders and files.

The inadvertent sharing of *existing* folders and files can have dangerous effects. Like inadvertent sharing of downloaded files, inadvertent sharing of existing files can make a user a high-volume uploader of infringing files. For example, a user might try to store downloaded files in his "My Documents" or "My Music" folder because these folders probably contain no existing files, only subfolders. Recursive sharing would then cause this user to "share" the thousands of audio files copied from purchased CDs stored in subfolders of "My Music."

But inadvertent sharing of existing files can also have other effects—thanks to a post-*Napster* change in the design of most filesharing programs. Napster, Inc.'s filesharing program shared only audio files. After the *Napster* litigation, distributors of filesharing programs were advised to bolster their capacity-for-substantial-noninfringing-use defense by redesigning their programs to share almost *all* types of files by default: "[I]f you're developing a file-sharing system or distributed search engine, support all file types, not just MP3 or Divx files."[36] Such advice was widely followed: KaZaA, LimeWire, BearShare, eDonkey, and Morpheus now share almost all types of files by default.

This changed behavior makes inadvertent sharing of existing files very dangerous. Most computers now store files containing highly sensitive information.[37] These files may contain sensitive personal information—credit card data, financial information, tax returns, scans of legal or medical records, digital photographs, personal correspondence, business documents, or other similar files. They may also contain sensitive information owned by an employer or another user of the computer. Inadvertent sharing of such files could result in identity theft, disclosure of trade secrets, economic espionage, or worse.[38]

Because inadvertent sharing of existing files and folders can have such serious consequences, it is critical to note how this problem was called to the attention of distributors of filesharing programs, how they responded, and what happened afterwards.

In the June 2002 study *Usability and Privacy: A Study of KaZaA P2P File-Sharing*, researchers Nathaniel Good and Aaron Krekelberg showed that users of the KaZaA filesharing program were sharing so many sensitive personal files that identity thieves had begun data-mining the KaZaA network for inadvertently shared credit-card data.[39]

To determine why users were sharing files inadvertently, *Usability and Privacy* developed four usability guidelines for responsible developers of filesharing programs and conducted a user study. The users studied were adults, and almost all of them were relatively sophisticated: All were regular computer users; all "were given a short tutorial on file sharing, and the concept of a shared folder"; and 83% had previously used filesharing programs.

Based upon the usability guidelines and the user study, *Usability and Privacy* concluded that KaZaA was unsafe. Its user interface was "weighted too heavily in favor of sharing files." *Usability and Privacy* revealed two features in the KaZaA interface that could cause users to share existing files inadvertently. These were the KaZaA share-folder and search-wizard features.[40]

The KaZaA share-folder feature was accessed from the program's "Options" menu. It would present the user with the following interface:

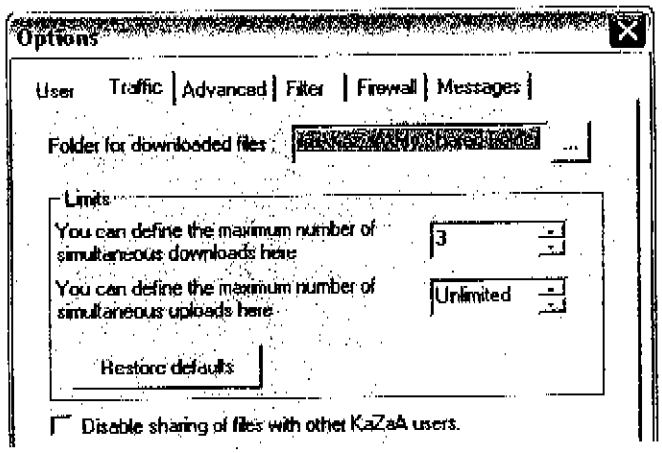

Figure 4: KaZaA 1.7.1

Usability and Privacy summarized the problems with the KaZaA share-folder feature: "The word "folder" is singular, implying one folder, and does not hint that all folders below it will be recursively shared with others." Worse still, "the name 'download folder' implies that it will be used to store files that are downloaded and has nothing to do with sharing. It does not mention that this folder (and the folders and files underneath) will also be shared with others...." Indeed, the KaZaA share-folder feature gave users only one obscure hint that the "download folder" might be shared: A checkbox near the bottom of the interface was labeled "Disable sharing of files with other KaZaA users."

The KaZaA search-wizard feature had changed over time. In versions before 1.7.1, the wizard could be accessed during the program's installation-and-setup process, (when the user would be most unfamiliar with the program), and from the "Options" menu within the installed program. In versions 1.7 to 2.4, the wizard could only be accessed from the "Options" menu within the program. It was inactive by default, but if activated by the user, it would produce a results screen like this one:

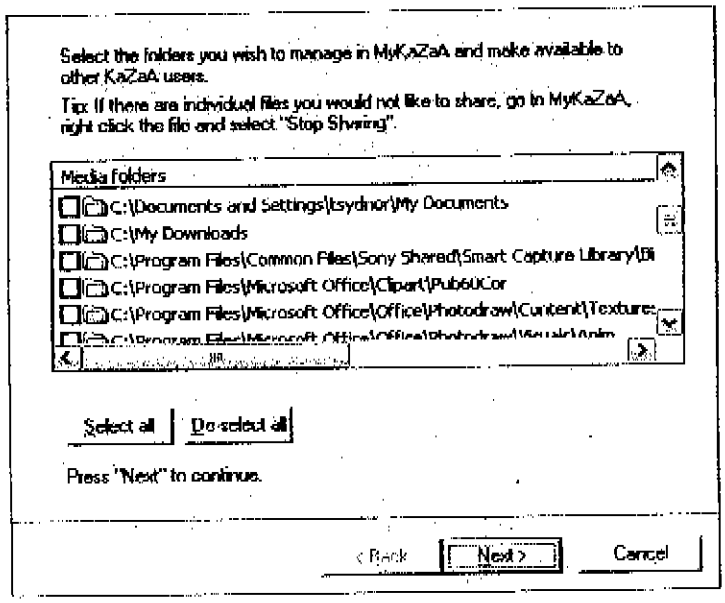

Figure 5: KaZaA 1.7.1

The results screen shown above shows the KaZaA search wizard "recommending" that the user share his "My Documents" folder. Note that "My Documents" will be shared only if the user checks the checkbox to the left of the folder path. But the user is not warned that "My Documents" will be shared recursively, and this information is essential if the user is to react intelligently to the absurd "recommendation" to share "My Documents."

Usability and Privacy cited many other problems with the results screen, including the following: (1) "it does not say what files in the 'My Documents' folder will be shared," (2) it "relies on the user's knowledge of what is capable of being shared by a file sharing program," and (3) "[i]t presumes that users have perfect knowledge of what kinds of files (and sub-directories with further files) are contained in these folders and that these

contents will be recursively shared." The study also confirmed that these presumptions did not correlate with reality: It noted, "Novice users are 'notoriously bad' at navigating hierarchical file structures," and it revealed that 75% of the users studied "believed that only multimedia files such as music, video and pictures could be shared."

Usability and Privacy concluded that "file sharing software is safe and usable if users ... are clearly made aware of what files are being offered for others to download [and] do not make dangerous errors that can lead to unintentionally sharing private files..." It concluded that KaZaA failed to satisfy these standards. It warned that "lessons learned from KaZaA are applicable to designers working with other P2P systems," and that "the potential violation of user privacy and the current abuses that we noted" meant that eliminating features that were causing inadvertent sharing of existing files "should be a top priority for file sharing applications...."

Because inadvertent sharing of existing files had such dangerous consequences, *Usability and Privacy* prompted two congressional hearings. During a hearing before the House Committee on Government Reform, staff investigators confirmed that thousands of users of filesharing programs were inadvertently sharing data files for popular finance-management software that could contain account numbers and detailed records about a user's finances.[41] During a hearing before the Senate Committee on the Judiciary, legislators repeatedly warned distributors that unless they eliminated features that caused users to share existing files inadvertently, their programs would compromise national security:

- "[I]n government agencies, employee use of P2P networks could ... disclose sensitive government data to the enemies of this country."
- "[I]f the user is a government employee ... sensitive government information could be made available to those unfriendly to the United States."
- "For government users, the situation is far worse. Not only personally sensitive information can be stolen, but information vital to the functioning of government, as well. Confidential memos, Defense Department information, law enforcement records, all could be available to any Internet user with some free software and the desire to go looking."[42]

In the aftermath of *Usability and Privacy* and the hearings, distributors of various filesharing programs were differently situated as to the problems identified. One needed only to refrain from adding features that had been shown to cause users to share existing files inadvertently. *Usability and Privacy* had noted that inadvertent sharing of sensitive files was less common on the Gnutella network. The design of the Gnutella-based program LimeWire may explain why: From at least the beginning of 2002 through June 2003, LimeWire contained neither a search-wizard nor a share-folder feature.

But most distributors of popular filesharing programs had deployed share-folder or search-wizard features. During the hearings, the distributors of KaZaA assured legislators, "[W]e welcome intelligent research like that done by Good and Krekelberg

and we always incorporate it into our product development plans."[43] They promised that the forthcoming release of KaZaA 2.5 would redress the identified problems.

After the hearings, other distributors claimed that they too had moved swiftly to redress inadvertent sharing of existing files. For example, on September 29, 2003, the distributors of Morpheus, BearShare, LimeWire, and eDonkey published a *Code of Conduct* that imposed the following obligations:

- "[Our] software and associated user instructions shall conspicuously require the user to confirm the folder(s) containing the file material that the user wishes to make available to other users before making such material available, and"
- "[Our] software and associated user instructions … shall be designed to reasonably prevent the inadvertent designation of the content of the user's … principal data repository … as material available to other users."[44]

On its face, the *Code* bars the use of KaZaA-like share-folder and search-wizard features on two separate grounds: Those features did not "conspicuously" require users to confirm that they wished to share all the folders that these features would actually share, and they were not designed "to reasonably prevent" sharing of a user's principal data repository. More importantly, the *Code*'s generally worded obligations also prohibit virtually any other feature that might cause inadvertent sharing—including, for example, a poorly disclosed redistribution feature.

Consequently, by September 29, 2003, the distributors of *all* of the programs studied in this report had declared that they would end the use of KaZaA-like share-folder or search-wizard features. These declarations also seemed credible: *Usability and Privacy* and the 2003 hearings had not treated misleading search-wizard and share-folder features as potential duping schemes. To the contrary, they were treated as mistakes in interface design that responsible distributors should correct.

Indeed, by mid 2004, distributors were claiming that they had responded so thoroughly that the problem of inadvertent sharing of existing files had become a mere "urban myth." On June 23, 2004, the distributors of Morpheus, BearShare, and eDonkey testified to a Senate Subcommittee that they had created "safeguards" that would "render the feared 'broadcast' of personal data to 'millions of others of Internet users' … wholly without foundation." They testified, "[A]s far as [we] are concerned, allegations that it is easy for a user to inadvertently 'publish' sensitive materials like … tax information through our software is literally the equivalent of an urban myth…."[45]

This same attitude also appears in the response that the distributors of BearShare, eDonkey, and Morpheus offered to a frequently-asked question about whether use of a filesharing program increases a user's risk of identity theft: "Absolutely nothing about peer-to-peer software itself … increases the odds that a user's personal information can or will be accessed by some unknown person."[46]